Non-State Actors and Norms of Responsible Behaviour in Cyberspace

Jacqueline Eggenschwiler

St Cross College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2020

Abstract

Computer systems and networks have become key determinants for the proper functioning of global markets, political institutions, and societies at large. Given their extensive reach into almost all areas of human activity, their safekeeping has become of strategic importance for a diverse range of actors. The proliferation of offensive cyberoperations, such as *WannaCry* or *Petya/NotPetya*, has spurred calls for normative measures of restraint, and behaviour-guiding *rules of the road*.

Despite surging numbers of academic publications pertaining to cybersecurity generally, and norm-making processes specifically, the contributions of non-state actors to global cybersecurity governance efforts have remained under-theorised.

With a view to offering correctives, this thesis examines the roles assumed by non-state actors in global cybersecurity norm formation processes. Specifically, it analyses how, in which capacities, and how effectively non-state protagonists engage in norm cultivation endeavours by surveying nine exploratory case studies, grouped into three stakeholder clusters, i.e. (a) civil society and academia, (b) corporate actors, and (c) expert communities.

Triangulating different qualitative means and methods of data collection and analysis, this thesis suggests that non-state actors have come to exert discernible politico-legal influence over discussions about norms of responsible behaviour in cyberspace. Advancing empirically more informed and varied conceptualisations of the parts played by non-state actors in cybersecurity norm creation projects, this dissertation suggests that their roles can be systematised along the following profiles: (a) knowledge brokers, (b) awareness raisers, (c) norm leaders and cooperation incubators, (d) diplomatic change agents, (e) discussion feeders and gap fillers, (f) implementation assistants and capacity builders, and (g) custom shapers.

The case studies reveal noteworthy variations in how non-state entities seek to shape actor behaviour and realise regulatory effects. The results of this inquiry go to show that non-state actors have to be taken seriously as key contributors to global cybersecurity steering efforts, and that their actions and authority have come to extend beyond advocacy or lobbying.

This thesis is dedicated to my family.

Acknowledgements

The rough and arguably premature ideas which stood at the beginning of this thesis would not have resulted in a comprehensive written body of work without the steady support of inspiring academics, encouraging friends, and loving family members.

Academically, I am deeply indebted to my supervisors Dr Rebecca Ann Williams and Dr Myriam Dunn Cavelty who have provided sage guidance, constructive feedback, and motivating advice throughout this endeavour. This thesis has benefited immensely from your academic rigour and foresight.

The many colleagues and friends whom I have had the pleasure of interacting with during lectures, presentations, and conferences also deserve a special thank you. You have provided important intellectual stimulus and feedback. I appreciate the thought and consideration you have given to reading and commenting on drafts of this manuscript.

The interview partners who have dedicated their time to answering my questions and have allowed me to gain access to practical insights also warrant my genuine gratitude. You have contributed much to empirically more grounded understandings of global cybersecurity norm formation processes.

I would also like to extend my appreciation to the staff and scholarly bodies who have supported this thesis administratively and financially: the Centre for Doctoral Training in Cyber Security, the Faculty of Law, and St Cross College.

Finally, the most heartfelt thank you goes out to my family for their unwavering love and support in every way. Without you, this academic journey would not have been possible.

Contents

List of Abbreviations

ANSSI	French National Agency for the Security of Information Systems (Agence Nationale de la Sécurité des Systèmes d'Information)
APC	Association for Progressive Communications
APNIC	Asia-Pacific Network Information Centre
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association of Southeast Asian Nations
Bitkom	Federal Association for Information Technology, Telecommunications and New Media (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)
(UN IGF) BPF	(United Nations Internet Governance Forum) Best Practice Forum
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CBM	Confidence Building Measures
(NATO) CCD COE	(North Atlantic Treaty Organisation) Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIA Triad	Confidentiality, Integrity, and Availability Triad
CoP	Community of Practice
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organisation
DDoS	Distributed Denial of Service
DNS	Domain Name System
EU	European Union
FIRST	Forum of Incident Response and Security Teams

G7	Group of Seven
G20	Group of 20
GCIG	Global Commission on Internet Governance
GCSC	Global Commission on the Stability of Cyberspace
GDP	Gross Domestic Product
(UN) GGE	(United Nations) Group of Governmental Experts
GPD	Global Partners Digital
GTI	Global Transparency Initiative
HCSS	Hague Centre for Strategic Studies
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
(UN) IGF	(United Nations) Internet Governance Forum
IGO	Inter-Governmental Organisation
INGO	International Non-Governmental Organisation
ISIS	Islamic State of Iraq and Syria
ISOC	Internet Society
ITU	International Telecommunications Union
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Cooperation and Development
(UN) OEWG	(United Nations) Open-ended Working Group
PLC	Programmable Logic Controller
PSIRT	Product Security Incident Response Team
S&P	Standard & Poor's
SCO	Shanghai Cooperation Organisation
SIGINT	Signals Intelligence
TCP/IP	Transmission Control Protocol/Internet Protocol
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
VoIP	Voice over Internet Protocol (IP Telephony)

Table of Primary Legal Sources

List of Figures

List of Tables

International norms in cyberspace are the product of, inter alia, negotiation and contestation over time in the context of evolving global practices, accompanying shifts in dynamic, underlying value systems that variously conflict and overlap, political compromise between multiple national and private interests, pragmatic agreements, serendipitous convergences, attempts at carrot-and-stick persuasion by the most powerful actors, and the socialisation of these same powerful agents. In short, they are the product of both chance and design, cooperation and conflict, emerging collective identities and changing conceptions of self-interest.

— Toni Erskine & Madeline Carr, *Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace (2016)*

1 Introduction

Contents

Advances in information and communication technologies (ICTs) over the past fifty years have contributed substantially to heightened degrees of economic growth and social innovation.[1] Transnational communication flows have increased at unprecedented rates, and information and data have become key resources, which in terms of their economic importance have been compared to commodities such as oil.[2] As levels of dependency on functioning infrastructures and networks for running and maintaining large numbers of 21st century economic, political, and social activities have increased, so have degrees of exposure to risks related to these technologies.

[1] James Manyika and Charles Roxburgh, *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity* (techspace rep, McKinsey & Company 2011) ⟨https://perma.cc/PUB4-EVB9⟩.

[2] The Economist, The World's Most Valuable Resource Is No Longer Oil, But Data (2017) ⟨https://perma.cc/MAZ9-QY4L⟩ accessed 21 May 2019.

Susceptible to manipulation and exploitation, digital infrastructures have been seen to provide nefarious actors with opportunities for malfeasance and rich canvasses for wrongdoing.[3] Assaults against public and private information and communication technologies by means of, for instance, Distributed Denial of Service (DDoS) attacks, or malware strikes (e.g. worms, viruses, ransomware, spyware, etc.) have risen steadily in numbers and levels of severity.[4] Indeed, malicious activities against network infrastructures have emerged as key hazards worldwide (see Figure 1.1).[5] Ranking among other major perils, such as extreme weather conditions, man-made environmental disasters, large-scale involuntary migration movements, water crises, and financial asset bubbles, cyberattacks have been attested extensive threat potentials, both in terms of likelihood of occurrence and impact.[6]

The surge in cybersecurity attacks has gone hand in hand with steep hikes in financial costs.[7] According to a study conducted by McAfee in conjunction with the Center for Strategic and International Studies, financial losses resulting from malicious activities carried out in and through cyberspace by governmental and non-governmental actors have grown from a projected USD 500 billion, or about 0.7% of global income to an estimated USD 600 billion, or 0.8% of global GDP between 2014-2018.[8] Among other

---

3 Joseph SJr Nye, 'Normative Restraints on Cyber Conflict' (Cambridge, MA, 2018) ⟨https://perma.cc/7TS9-CG8G⟩; Brian M Mazanec, 'Conclusions and Recommendations' in *The Evolution of Cyber War* (University of Nebraska Press 2015); Jan-Frederik Kremer and Benedikt Müller, *Cyberspace and International Relations* (Jan-Frederik Kremer and Benedikt Müller eds, Springer Berlin Heidelberg 2014) ⟨https://perma.cc/6Y94-7WY7⟩.

4 BDO, *Top Ten Trends and Key Reccommendations for 2019* (techspace rep, 2018) ⟨https://perma.cc/RUK7-YBBM⟩; BDO, *Cyber Security in 2020: Top Ten Predictions and Recommendations* (techspace rep, 2019) ⟨https://perma.cc/5TD3-LHVL⟩; Center for Strategic and International Studies, *Significant Cyber Incidents Since 2006* (techspace rep, 2019) ⟨https://perma.cc/PP76-EQA5⟩.

5 World Economic Forum, *The Global Risks Report 2020* (techspace rep, World Economic Forum 2020) ⟨https://perma.cc/TJ9K-TXSJ⟩.

6 Ibid.

7 Accenture and Ponemon Institute, *Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection* (techspace rep, 2019) ⟨https://perma.cc/LQ77-MW9H⟩.

8 James Lewis, *Economic Impact of Cybercrime – No Slowing Down* (techspace rep, McAfee 2018) ⟨https://perma.cc/J987-TUS8⟩.

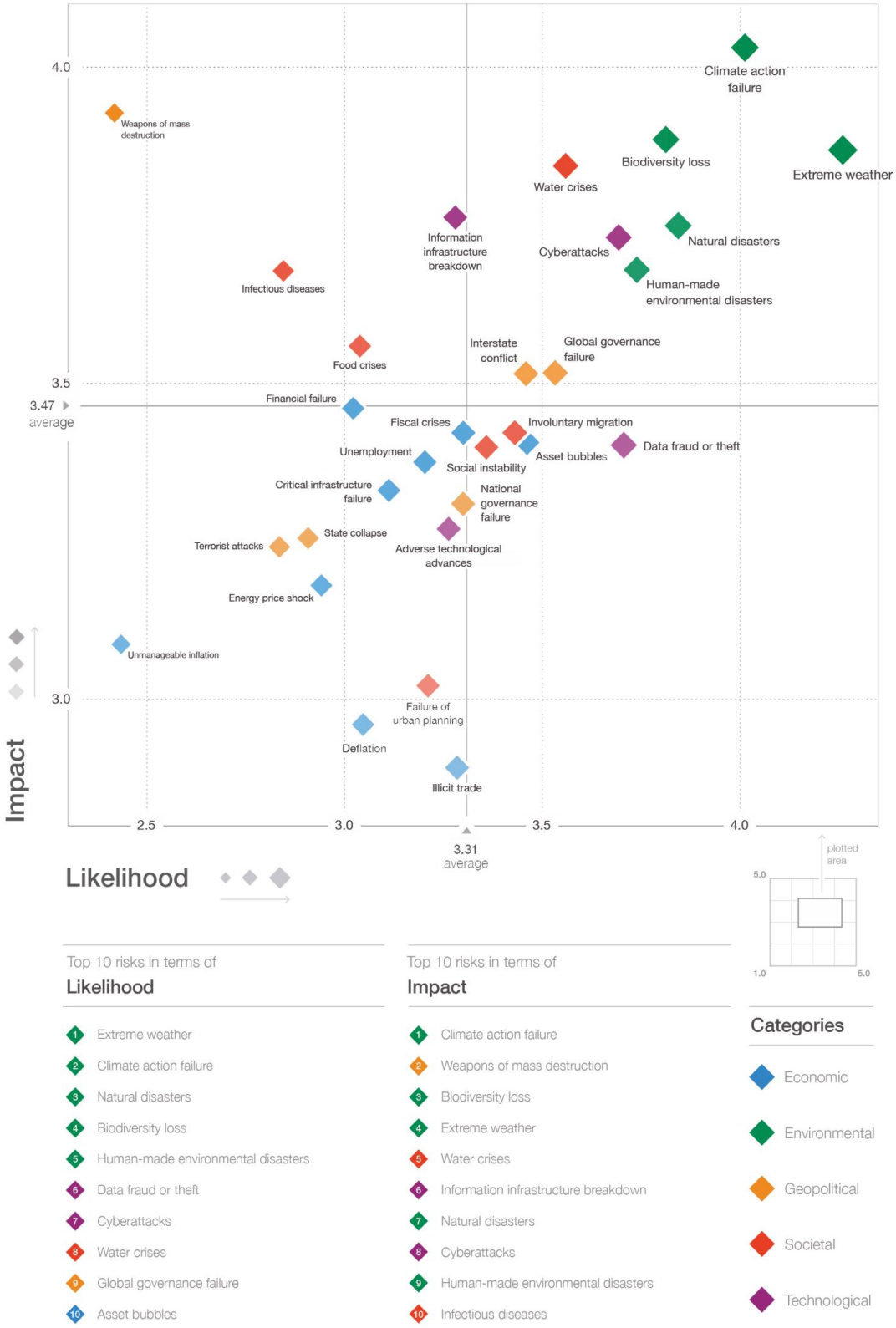

Figure 1.1: World Economic Forum Global Risks Landscape 2020, see World Economic Forum, *The Global Risks Report 2020* (techspace rep, World Economic Forum 2020) ⟨https://perma.cc/TJ9K-TXSJ⟩.

things, the study cited higher adoption rates of new technologies by cybercriminals, budding numbers of new users online, enhanced service portfolios, e.g. cybercrime-as-a-service, new offensive hubs, as well as growing financial sophistication among perpetrators as main reasons for the escalation of monetary losses.[9]

The proliferation of cybersecurity incidents has also had negative effects on aspects of trust, privacy, and freedom from fear.[10] As per research presented by Ipsos, the Centre for International Governance Innovation, the United Nations Conference on Trade and Development, and the Internet Society (ISOC), more than 50% of internet users worldwide expressed heightened degrees of concern about their online privacy in 2018 compared to 2017.[11] They also stated amplified levels of distrust vis-à-vis social media platforms, search engines, and internet technology companies.[12] Trust in government agencies, e.g. concerning adequate protection of personal data, also experienced a setback.[13]

Against the background of burgeoning cybersecurity incidents, increasing levels of socio-economic dependence, and continuously growing attack surfaces, questions regarding the stability and safekeeping of cyberspace have attained considerable policy relevance and have sparked wide-ranging discussions among public and private entities.[14]

---

9 Lewis (n 8).

10 Ibid.

11 United Nations Conference on Trade and Development, Data Privacy: New Global Survey Reveals Growing Internet Anxiety (2018) ⟨https://perma.cc/NGT3-RHNC⟩ accessed 26 February 2019.

12 Darrell Bricker, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust* (techspace rep, Ipsos 2018) ⟨https://perma.cc/Z4TA-LACZ⟩.

13 Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity* (techspace rep, Pew Research Center 2017) ⟨https://perma.cc/P55P-SR7R⟩; Camino Kavanagh and Daniel Stauffacher, *A Role for Civil Society in Cybersecurity Affairs* (techspace rep, ICT4Peace Foundation 2014) ⟨https://perma.cc/57TS-WEG9⟩.

14 Mark Raymond, 'Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot' [2016] Strategic Studies Quarterly 123 ⟨https://perma.cc/K39C-PDSB⟩; Nazli Choucri and David D Clark, 'Integrating Cyberspace and International Relations: The Co-Evolution Dilemma' [2012] (29) SSRN Electronic Journal 1 ⟨https://perma.cc/9LZ8-SLGA⟩.

In concurrence with these developments, calls for effective steering mechanisms and behaviour-guiding rules of the road pertaining to the digital domain have grown louder.

1.1 Context and Problem Setting

First discussions concerning the creation of instruments for curbing and remediating negative consequences resulting from networked systems and infrastructures, began to surface as early as 1996.[15] In 1996, the Council of the European Union, endorsed a bid put forward by the French government which sought to initiate a *Charter for International Cooperation on the Internet*.[16] At the time, 'the French Minister for Information Technology expressed hope that the initiative would eventually lead to an accord comparable to the international law of the sea', i.e. a set of legally binding provisions, laying out the rights and obligations of state parties in maritime matters, or digital matters, respectively.[17]

Equally concerned about nefarious applications of ICTs, in 1998, the Russian government brought the rapid developments pertaining to information and communication technologies and their potentially destabilising effects on states and matters

---

15 Kristen E Eichensehr, 'The Cyber-Law of Nations' (2015) 103(2) Georgetown Law Journal 317 ⟨https://perma.cc/W58Z-SHYU⟩.

16 Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) 30(4) Leiden Journal of International Law 877 ⟨https://perma.cc/498K-JFJV⟩.

17 Timothy S Wu, 'Cyberspace Sovereignty? The Internet and the International System' (1998) 10(3) Harvard Journal of Law & Technology 647 ⟨https://perma.cc/4LEU-KQB4⟩, 660. Questions regarding the law of the sea are regulated by the United Nations Convention on the Law of the Sea, which entered into force in 1994. 'Up to the middle of the 20th century the law of the sea was mainly customary. The growing complexity of interests, reflected in unilateral claims and in the resistance or in the partial acceptance they met with, and the need to obtain a measure of stability through a multilateral approach, brought about the need to go beyond customary law through the process of codification', see Treves Tullio, 'Law of the Sea' in *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2011) ⟨https://perma.cc/WD4W-TR9A⟩ 11. With this in mind, it is fair to say that the international law of the sea holds some analogical relevance for cyberspace.

of international security to the attention of the United Nations (UN).[18]

In reaction to Moscow's repeated undertakings in the remit of the United Nations General Assembly's First Committee on Disarmament and International Security, the Secretary-General called to life a *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN GGE) to study existing and emerging threats emanating from the virtual realm and possible cooperative measures to address them.[19]

The first group composed of 15 governmental representatives, appointed on the basis of equitable geographical distribution, began its work in 2004.[20] Since 2004, six UN GGEs of different compositions have been established.[21] Undermined by stark

---

[18] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (1998) ⟨https://perma.cc/SV8C-6Q53⟩. Moscow's motivations for debating issues concerning global ICTs in the context of the United Nations emerged in consideration of a perceived Western dominance in cyberspace, see Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee* (techspace rep, ICT4Peace Publishing 2012) ⟨https://perma.cc/VS34-DPXX⟩; Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5(1) Journal of Cybersecurity 1 ⟨http://perma.cc/654V-FWKL⟩.

[19] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2003) ⟨https://perma.cc/SY9J-7VFC⟩; Fen Osler Hampson and others, *Getting Beyond Norms: New Approaches to International Cyber Security Challenges* (techspace rep, Centre for International Governance Innovation 2017) ⟨https://perma.cc/U8YX-ABDW⟩. Following its initial submission to the General Assembly in 1998, Moscow tabled similar proposals in the years ensuing 1998, e.g. A/Res/54/49 (1999); A/Res/55/28 (2000); A/Res/56/19 (2001), and A/Res/56/19 (2002), see United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (1999) ⟨https://perma.cc/BM5B-M93Z⟩; United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2000) ⟨https://perma.cc/4K4W-KV4N⟩; United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2001) ⟨https://perma.cc/9GLP-XKNN⟩; United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2002) ⟨https://perma.cc/4ZZJ-995B⟩.

[20] The nations represented in the first Group of Governmental Experts included Belarus, Brazil, China, France, Germany, India, Jordan, South Korea, Malaysia, Mali, Mexico, Russia, South Africa, the United Kingdom, and the United States, see Camino Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (Geneva, 2017) ⟨https://perma.cc/ZT92-6GEA⟩.

[21] The first UN GGE met in 2004-2005, the second convened in 2009-2010, the third group held meetings in 2012-2013, the fourth UN GGE gathered in 2014-2015, the fifth group assembled in

ideological differences concerning central concepts under discussion, the first group concluded its meetings without results.[22]

Subsequent to the failure of the first UN GGE to produce meaningful outcomes, the Secretary General appointed a second group to resume the work of the first group in 2009. In the wake of large-scale cyberattacks in Estonia and Georgia in 2007 and 2008, respectively, the second Group of Governmental Experts was able to make more headway, and produce a short consensus report.[23] The events in Estonia and Georgia helped increase awareness among governments about the tangible security risks associated with ICTs. The attacks on Estonia also served as vivid illustrations for how 'the absence of international agreement on the most basic governing principles in cyberspace' augment the potentials for escalation and conflictuous relations.[24]

Apropos enacting steering mechanisms for the virtual realm, the 2010 UN GGE report merely proposed to consider

> (i) [f]urther dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure; (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict; (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; (iv) Identification of measures to support capacity-building in less developed countries; (v) Finding possibilities to elaborate

---

2016-2017, and the sixth UN GGE was initiated in 2019. Cumulatively these six groups have issued a total of three consensus reports (so far).

22 As stated by the Chairman of the 2004-2005 UN GGE, Ambassador Andrey Krutskikh, '[e]ven with the use of translation, the members of the Group of Governmental Experts spoke different languages with respect to essential issues related to international information security, because the international community has still not developed unified and generally accepted definitions of key terms and concepts in that area', see United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2005) ⟨https://perma.cc/XGY6-SSZY⟩ 5.

23 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, 2010) ⟨https://perma.cc/LSD7-2YE7⟩.

24 Henriksen (n 18) 2.

common terms and definitions relevant to General Assembly resolution 64/25.[25]

The 2012-2013 and 2014-15 iterations that followed the 2009-2010 UN GGE, managed to bring more granularity and depth to debates about developments in the field of information and communication technologies in the context of international security, particularly with regard to norms of responsible behaviour.[26] The consensus reports issued by the 2012-2013 and 2014-15 UN GGEs maintained that international law, and in particular the United Nations Charter, apply and have to be observed in cyberspace.[27] The consensus document of the 2014-15 group further proposed eleven norms of responsible state behaviour.

Among other things, the report held that states should not knowingly allow their territory to be used for internationally wrongful acts employing cybermeans or support activities that intentionally damage critical infrastructure, including other states' computer emergency response teams (CERT/CSIRT).[28] Furthermore, it stipulated that they should ensure supply chain security, and cooperate to prevent harmful practices in the use of digital technologies. To increase stability and security, the report also suggested that states should respond to appropriate requests for assistance by other

---

[25] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 23) 18.

[26] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, 2013) ⟨https://perma.cc/X28E-M84A⟩; United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, A/70/174, 2015) ⟨https://perma.cc/KDE8-33PM⟩.

[27] NATO Cooperative Cyber Defence Centre of Excellence, United Nations Group of Governmental Experts' Long-Awaited Report on Maintaining Peace and Stability of the ICT Environment (2013) ⟨https://perma.cc/86B7-6KYL⟩ accessed 18 January 2019.

[28] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26).

states and engage in responsible reporting of vulnerabilities.[29]

The 2016-17 edition of the UN GGE was intended to build on the achievements of the preceding UN GGEs, and to further elaborate on the provisions contained in the consensus documents issued by the 2012-2013 and 2014-15 gatherings.[30] However,

---

[29] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26); NATO Cooperative Cyber Defence Centre of Excellence, 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law (2015) ⟨https://perma.cc/9558-MZ42⟩ accessed 18 January 2019. The list of norms stipulated as part of the 2015 consensus report included the following provisions: '(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security; (b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences; (c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; (d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect; (e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression; (f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public; (g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions; (h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty; (i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; (j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure; (k) States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorised emergency response teams to engage in malicious international activity', see United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26) 7-8.

[30] Endeavours to construct norms and build confidence among sovereign actors in response to ICT-related insecurities have also taken place outside the confines of the United Nations, i.e. in fora including the African Union, the ASEAN Regional Forum, the Brazil, Russian Federation, India, China and South Africa (BRICS) grouping, the Council of Europe, the European Union,

discussions proved to be more contentious and ideologically charged, and failed to bring about substantive agreement on issues including the applicability of the right to self-defence and international humanitarian law.[31]

What ensued the 2017 setback of the UN GGE was a phase of sovereign retreat and a noticeable surge in the numbers of non-state actor initiatives.[32] Examples of non-state actor proposals launched following the non-consensus outcome included among others, the University of Leiden's and ICT4Peace Foundation's co-sponsorship of a *Global Commentary on Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology*, Microsoft's proposal for a *Digital Geneva Convention*, its adoption of a *Cybersecurity Tech Accord*, its initiation of a *Digital Peace Now* campaign, its backing of the *Paris Call for Trust and Security in Cyberspace*, as well as its launch of a *CyberPeace Institute*, Siemens' conclusion of a *Charter of Trust*, Kaspersky Lab's unveiling of a *Global Transparency Initiative*, the second International Group of Experts' release of the *Tallinn Manual 2.0*, as well as the Global Commission on the Stability of Cyberspace's (GCSC) calls for the *Protection of the Public Core of the Internet*, the safeguarding of electoral infrastructures, and the release of the *Norm Package Singapore*.[33]

---

the Group of Seven (G7), the Group of 20 (G20), the Organization of American States, the Organization for Economic Cooperation and Development (OECD), the Organization for Security and Cooperation in Europe (OSCE), and the Shanghai Cooperation Organization (SCO), see Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (n 20) 11.

31 Henriksen (n 18).

32 Alex Hern, WannaCry, Petya, NotPetya: How Ransomware Hit the Big Tme in 2017 (2017) ⟨https://perma.cc/CNC7-ZSCR⟩. UN-based discussions only started to resurface again in late 2018, when the United Nations General Assembly passed two separate, and procedurally competing resolutions relating to responsible behaviour in cyberspace: (a) A/RES/73/27 submitted by Moscow, and (b) A/RES/73/266 sponsored by Washington, see United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (2018) ⟨https://perma.cc/5RGC-UCSK⟩; United Nations General Assembly, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (2018) ⟨https://perma.cc/3TU5-GJX9⟩.

33 Eneken Tikk and others, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (Eneken Tikk ed,

With regard to theory and practice, state-led efforts directed at constructing rules of the road for the virtual realm have long enjoyed analytical primacy over non-state actor efforts. However, as governments continue to grapple with conflicting national interests, reciprocal distrust, and reaching baseline agreements on normative prescriptions, it is critical to survey normative efforts emerging in the shadows of public endeavours.[34]

1.2 Research Question and Contributions

Non-state actors have been central to the rise and advancement of cyberspace. As developers of products and suppliers of services such as endpoint protection and threat analysis, non-state actors, including large multinational corporations as well as individual academic researchers, such as Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, or Tim Berners-Lee, have made important contributions to the security and overall design of the virtual realm.[35] Furthermore, as owners and

United Nations Office for Disarmament Affairs 2017) ⟨https://perma.cc/N6KK-GKLT⟩; Brad Smith, The Need For a Digital Convention (2017) ⟨https://perma.cc/4J63-P45T⟩ accessed 9 July 2018; Brad Smith, 34 Companies Stand Up for Cybersecurity with a Tech Accord (2018) ⟨https://perma.cc/J3MH-559K⟩ accessed 10 July 2018; Cybersecurity Tech Accord, About the Cybersecurity Tech Accord (2019) ⟨https://perma.cc/6M78-2ZTQ⟩ accessed 19 August 2019; CyberPeace Institute, Working Towards a Safer Online World for All (2019) ⟨https://perma.cc/D7VV-JRG5⟩ accessed 17 November 2019; Charter of Trust, Charter of Trust: For a Secure Digital World (2018) ⟨https://perma.cc/ZNQ6-UCZ5⟩ accessed 11 July 2018; Kaspersky Lab, Our First Transparency Center Will Be in Switzerland (2018) ⟨https://perma.cc/SM8R-VKMX⟩ accessed 16 May 2018; Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (techspace rep, 2018) ⟨https://perma.cc/SJB5-5YZP⟩.

[34] Leonie Maria Tanczer, Irina Brass, and Madeline Carr, 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy' (2018) 9(3) Global Policy 60 ⟨https://perma.cc/KV4X-6LMM⟩.

[35] Roxana Radu, 'Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace' in Jan-Frederik Kremer and Benedikt Müller (eds), *Cyberspace and International Relations* (Springer Berlin Heidelberg 2014) ⟨https://perma.cc/SQ6Z-PVTC⟩; Scott J Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press 2014); Leslie Daigle, 30 Years of TCP and IP on Everything (2013) ⟨https://perma.cc/D94R-U79L⟩ accessed 28 February 2018; Barry M Leiner and others, 'A Brief History of the Internet' (2009) 39(5) ACM SIGCOMM Computer Communication Review 22 ⟨https://perma.cc/KR8K-6KR4⟩.

operators of large parts of critical network infrastructures and technology platforms, they have come to wield considerable influence over key aspects of cyberspace and human existence. 'Internet companies have become central platforms for discussion and debate, information access, commerce and human development'.[36]

While scholarly endeavours pertaining to cybersecurity generally, and norm-making processes specifically have surged over the past years, surprisingly little comprehensive work has been conducted on analysing the contributions of (non-malicious) non-state actors to discussions about rules of the road for global information and telecommunications infrastructures in a systematically and analytically rigorous manner.[37]

Although recognised as entities under international law and international relations, non-state actors have been treated with considerable theoretical ambiguity.[38] Beyond attesting their empirical existence and advocacy activities, political and legal scholarship have provided scant evaluations of the roles taken on by non-state actors in global steering and norm formation processes pertaining to cybersecurity. As aptly stated by D'Aspremont,

---

[36] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (techspace rep, A/HRC/38/35, 2018) ⟨https://perma.cc/4PYE-S97W⟩ 5.

[37] Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (n 20); Joseph SJr Nye, 'The Regime Complex for Managing Global Cyber Activities' (Paper Series, Centre for International Governance Innovation and Chatham House 2014) ⟨https://perma.cc/3L4P-Z2LP⟩; Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace' (2014) 36(5) American Foreign Policy Interests 322 ⟨https://perma.cc/934D-ERHN⟩; Toni Erskine and Madeline Carr, 'Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace' in Anna-Maria Osula and Henry Rõigas (eds), *Legal, Policy & Industry Perspectives* (NATO Cooperative Cyber Defence Centre of Excellence 2016) ⟨https://perma.cc/S39A-6786⟩; Brian M Mazanec, 'Constraining Norms for Cyber Warfare Are Unlikely' (2016) 17(3) Georgetown Journal of International Affairs 100 ⟨https://perma.cc/DC74-BH33⟩; Eneken Tikk-Ringas, 'International Cyber Norms Dialogue as an Exercise of Normative Power' (2016) 17(3) Georgetown Journal of International Affairs 47 ⟨https://perma.cc/J33H-KFA9⟩; Julie J C H Ryan, Daniel J Ryan, and Eneken Tikk, *Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation* (techspace rep, 2010) ⟨https://perma.cc/KCJ8-G3ZS⟩; Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View* (techspace rep, Hoover Institution 2011) ⟨https://perma.cc/4PYY-HFT9⟩.

[38] Math Noortmann and Cedric Ryngaert, *Non-State Actor Dynamics in International Law: From Law-Takers to Law-Makers* (Math Noortmann and Cedric Ryngaert eds, Routledge 2016).

> the roles and status of non-state actors ... remain a topic of significant complexity, for they simultaneously raise conceptual as well as dynamic issues. On the one hand, ... [their] activities (and the normative outcomes of their actions) cannot entirely be caught by the net that international legal scholars have fabricated to catch reality, and definitely do not fall under the existing formal categories of international law. On the other hand, non-state actors shed new light on the dynamics of international law-making and international law-enforcement, which have long been underestimated in a state-centric normative system.[39]

With the intention of extending existing frames of reference, and addressing gaps in bodies of scholarly literature, this thesis responds to the following research question:

How and in which capacities do non-state actors contribute to global norm construction efforts pertaining to responsible behaviour in cyberspace, and how effective is their engagement?

This thesis is premised on the view that 'normative authority at the international level is no longer exercised by a closed circle of high-ranking officials acting on behalf of states, but has instead turned into an aggregation of complex procedures involving non-state actors'.[40] As such, attaining a better grasp of the roles and responsibilities taken on by non-state actors in global cybersecurity norm formation processes is key for understanding contemporary patterns of governance and forms of control relating to the virtual realm.

While not disputing the significance of public actors in enacting and enforcing rules of the road for the digital domain, this monograph argues that focusing on states alone only provides a partial picture of the forces at work in global steering and norm

---

[39] Jean D'Aspremont, *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law* (Jean D'Aspremont, William Michael Reisman, and Math Noortmann eds, Routledge Research in International Law, Routledge 2011) 1.

[40] Jean D'Aspremont, *Formalism and the Sources of International Law: A Theory of the Ascertainment of Legal Rules* (Oxford University Press 2013) 2.

creation efforts.[41] New empirical realities and governance structures have emerged which span multiple levels of interaction, involve various regulatory instruments, and rely on the contributions of a great variety of different stakeholders.[42]

International relations and international law have served as key lenses through which to examine processes of global norm construction and implementation.[43] Building on existing scholarship in these areas, and extending analytical frameworks, this thesis

---

41 Against the background of rising numbers of and activities conducted by non-state actors, some scholars have sought to reconceptualise the roles of governments in decentralised, pluralised, or networked regulatory settings, see, for instance, Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) Social Media Society 1 ⟨https://perma.cc/972B-TAM7⟩; Adam Crawford, 'Networked Governance and the Post-Regulatory State?' (2006) 10(4) Theoretical Criminology 449 ⟨http://perma.cc/N598-VQ2C⟩; Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54(1) Current Legal Problems 103 ⟨https://perma.cc/6XKU-KDYK⟩; Christine Parker, 'The Pluralization of Regulation' (2008) 9(2) Theoretical Inquiries in Law ⟨http://perma.cc/RX3H-52RL⟩; Scott C Burris, Peter Drahos, and Clifford D Shearing, 'Nodal Governance' (2005) 30 Australian Journal of Legal Philosophy 1 ⟨https://perma.cc/2GTR-H69Q⟩. With regard to cybersecurity, broadening dominating perceptions of global ordering requires '[accounting] for ... diverse, contested environment[s] of agents with differing levels of power and visibility: users, algorithms, platforms, industries and governments', see Kate Crawford and Catharine Lumby, 'Networks of Governance: Users, Platforms, and the Challenges of Networked Media Regulation' eng (2013) 1(3) International Journal of Technology Policy and Law 270 ⟨http://perma.cc/B2XW-YZHB⟩, 9.

42 Michael Zürn, 'Global Governance as Multi-Level Governance' in David Levi-Faur (ed), *The Oxford Handbook of Governance* (Oxford University Press 2012) ⟨https://perma.cc/QK5N-8MD7⟩; Kenneth W Abbott and Duncan Snidal, 'The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State' in Walter Mattli and Ngaire Woods (eds), *The Politics of Global Regulation* (Princeton University Press 2009) ⟨https://perma.cc/7DCF-KZFV⟩; Nye, 'The Regime Complex for Managing Global Cyber Activities' (n 37); Carnegie Endowment for International Peace, Cyber Norms Revisited: International Cybersecurity and the Way Forward (2017) ⟨https://perma.cc/W89H-ZL53⟩ accessed 9 November 2017.

43 Ann Florini, 'The Evolution of International Norms' (1996) 40(3) International Studies Quarterly 363 ⟨https://perma.cc/J7ZW-Y3HG⟩; Kendall Stiles and Wayne Sandholtz, 'Cycles of International Norm Change' in Kendall Stiles and Wayne Sandholtz (eds), *International Norms and Cycles of Change* (Oxford University Press 2008); Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998) 52(4) International Organization 887 ⟨https://perma.cc/7CWG-H7JE⟩; Jean D'Aspremont, 'International Law-Making by Non-State Actors: Changing the Model or Putting the Phenomenon into Perspective?' [2010] SSRN Electronic Journal 171 ⟨https://perma.cc/7LSN-2XXX⟩; John Gerard Ruggie, *The Social Construction of the UN Guiding Principles on Business and Human Rights* (techspace rep, Harvard Kennedy School 2017) ⟨https://perma.cc/F3QN-VPTB⟩; Matthew J Hoffmann, 'Norms and Social Constructivism in International Relations' in *Oxford Research Encyclopaedia of International Studies* (Oxford University Press 2017) ⟨https://perma.cc/DY7C-DU6J⟩; Julia Black, ''Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes' (2017) 9(2) International Theory 286 ⟨https://perma.cc/3Y2Z-GEBC⟩; Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (February, London, 2008) ⟨https://perma.cc/6W4J-NKKV⟩.

lays important groundwork for thinking about the contours of global cybersecurity governance arrangements in an interdisciplinary fashion. It comments on the characteristics of different non-state actor schemes, highlights areas of ownership and influence, and unveils the modes of social coordination through which non-state protagonists seek to shape actor behaviour in the digital realm.[44] In light of increasing levels of urgency surrounding efforts directed at responding to abuses of information and communications technologies, there is a pressing need for scholarly explorations addressing questions of regulatory inputs and responsibilities.[45]

This dissertation makes several important analytical as well as practical contributions. In terms of analytical contributions, it adds to more recent endeavours in the disciplines of international relations and international law, which have set out to 'push beyond ontological claims of state-centrism by providing theoretical bases for attention to other types of actors'.[46] It challenges positivist, state-centric notions underlying international relations and international law literatures, opens up and develops analytical frameworks, and highlights the importance of ideational factors in regulating issues of global proportions.[47] Questioning traditional logics of

---

[44] Shaun Breslin and Helen ES Nesadurai, 'Who Governs and How? Non-State Actors and Transnational Governance in Southeast Asia' (2018) 48(2) Journal of Contemporary Asia 187 ⟨https://perma.cc/XP74-3MLF⟩.

[45] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) The American Journal of International Law 425 ⟨https://perma.cc/QB6N-SZC3⟩; Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (2016) 21(3) Journal of Conflict and Security Law 455 ⟨https://perma.cc/924K-AAJ8⟩; Johan Sigholm, 'Non-State Actors in Cyberspace Operations' (2013) 4(1) Journal of Military Studies 1 ⟨https://perma.cc/7EKB-UZR9⟩; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) Journal of Conflict and Security Law 429 ⟨https://perma.cc/N358-6C9L⟩.

[46] Martha Finnemore, 'New Directions, New Collaborations for International Law and International Relations' in Thomas J Biersteker, Peter J Spiro, and Chandra Lekha Sriram (eds), *International Law and International Relations* (Routledge 2006) 274.

[47] David Weissbrodt, 'Roles and Responsibilities of Non-State Actors' in Dinah Shelton (ed), *The Oxford Handbook of International Human Rights Law* (Oxford University Press 2013) ⟨https://perma.cc/YYU7-PLVQ⟩; Markus Kornprobst, 'Non-State Actors in International Relations: Actors, Processes, and an Agenda for Multifaceted Dialogue' in *Non-State Actors in International Law* (Hart Publishing 2015) ⟨https://perma.cc/22N2-K8MB⟩.

agency, it provides more granular depictions of the participants present in global steering efforts. It also offers more nuanced evaluations of the social, legal, and political processes and practices at work with regard to ensuring the security and stability of the digital domain.[48]

Conceptually, this thesis also adds to more fine-grained understandings of the different steering parts executed by non-state actors. The roles of non-traditional security agents in the digital domain have remained under-theorised and have frequently and unsuitably been reduced to advocacy and lobbying endeavours.[49] By surveying various non-state actor undertakings concerned with cultivating norms of responsible behaviour for the virtual realm, this thesis contributes to enhanced understandings of private contributions to global steering processes, and offers analytical grids which can be applied to subsequent (case) investigations.

Besides generating stocks of data concerning non-state actor contributions to global cybersecurity governance processes, this thesis also offers relevant tools for structuring and making sense of non-state actor activities. The instruments developed as part of this thesis help reveal differences in both quality and success relating to the norm creation efforts undertaken by non-governmental entities. They are coupled to theoretical debates about new modes of governance in international relations, as well as practical concerns about the effects of these new forms of steering on global policy deliberations and international cooperation more generally.[50]

---

48 Jérémie Cornut, 'The Practice Turn in International Relations Theory' in *Oxford Research Encyclopedia of International Studies* (Oxford University Press 2015) ⟨https://perma.cc/V8Q6-DAZD⟩.

49 Breslin and Nesadurai (n 44).

50 Cornelia Ulbert, 'How to Hit a Moving Target: Assessing the Effectiveness of Public-Private Partnerships' in Hendrik Hegemann, Regina Heller, and Martin Kahl (eds), *Studying 'Effectiveness' in International Relations: A Guide for Students and Scholars* (Verlag Barbara Budrich 2012). According to Ulbert, governance commitments by private actors have often been considered to be 'more *effective* than the activities of traditional state actors, because they operate in a more *businesslike* way, see ibid'. However, to determine relevant degrees of truth, it is necessary to operationalise considerations of effectiveness, and compare.

Furthermore, by probing more deeply into the governing roles of non-state actors, this thesis also sheds light on how values are allocated at the global level, and spells out who is involved in the allocation of these values respectively.[51] Likewise, it shows how accountability and legitimacy are sought by non-governmental protagonists and comments on the implications of their norms-oriented ventures on cybersecurity governance structures.[52]

In addition to examining active construction processes in heterogeneous and contested normative environments, this thesis draws attention to the possibilities of quasi-legal instruments to produce law-like effects. It demonstrates the validity of alternative regulatory approaches, including soft law and political commitments to coordinate and order global problem settings.[53] 'Proponents of soft law have long trumpeted the compliance pull of [legally] non-[binding] norms, but to date, international law as a discipline has given relatively little attention to the processes by which such norms garner authority'.[54]

In terms of empirical contributions, this thesis presents comprehensive primary evidence of the influence exerted by non-state actors on global norm creation processes pertaining to the digital domain. It lets policymakers appreciate that, as non-state actors continue to be concerned about immediate and future threats to political, economic, and social systems resulting from the misuse of information and communications technologies, and seek regulatory engagement, it is important to

---

51 Breslin and Nesadurai (n 44); John Gerard Ruggie, 'Reconstituting the Global Public Domain - Issues, Actors, and Practices' (2004) 10(4) European Journal of International Relations 499 ⟨https://perma.cc/W6T5-BATR⟩.

52 Naghmeh Nasiritousi, *Shapers, Brokers and Doers: The Dynamic Roles of Non-State Actors in Global Climate Change Governance* (Linköping University 2016) ⟨https://perma.cc/D892-CQQ2⟩.

53 Finnemore and Hollis (n 45) 478.

54 Ibid 429.

reconsider existing forms of interaction and cooperation among governmental and non-governmental entities.[55] 'The distributed and layered nature of cyberspace, particularly the internet, suggests that efforts to respond to current global ICT ... insecurities requires significant collaboration and cooperation among different actors at different levels and across borders'.[56]

This thesis puts forward that in order to move from cyberinsecurity to more cyberstability, and to effectively respond to large-scale cybersecurity incidents, such as WannaCry or Petya/NotPetya, it is critical for governmental structures and regulatory systems to interact with non-governmental systems in a more symbiotic and integrated fashion.[57]

> [T]he roles of non-state actors are continuously evolving and depend on the changing nature of relations between state and non-state actors as well as efforts by non-state actors to expand their policy space[s] by justifying and seeking recognition for their participation.[58]

Overall, this thesis can be read both as an analytically-structured and comprehensive compilation of case studies examining and revealing the broad spectrum of roles taken on by non-state actors in cybersecurity-related regulatory projects (which are not captured by traditional frames of international law and international relations), and/or as a set of empirical instances which demonstrate the significance of non-state actors in the creation of norms-based global governance regimes.

While endeavouring to be as comprehensive as possible in answering the research question formulated earlier, it is beyond the scope of this inquiry to survey the entire

---

55 Hampson and others (n 19); Jason Healey, *Innovation on Cyber Collaboration: Leverage at Scale* (techspace rep, Atlantic Council 2018) ⟨https://perma.cc/ZH4B-8UPY⟩.

56 Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (n 20) 9.

57 WannaCry, Petya, NotPetya: How Ransomware Hit the Big Tme in 2017 (n 32); Alex Hern, Ransomware Attack ot Designed to Make Money, Researchers Claim (2017) ⟨https://perma.cc/6M3N-33XK⟩ accessed 28 May 2018.

58 Nasiritousi (n 52) 40.

spectrum of global norm-building activities undertaken by non-state actors in the virtual realm. Instead, this dissertation focuses on nine case studies, grouped into three stakeholder clusters: (a) civil society and academia, (b) corporate actors, and (c) expert communities.

1.3 Research Design and Scope

Methodologically, this thesis represents a cross-disciplinary, empirically-informed body of work, which draws on insights from international relations and international law. 'Crisscrossing research between international relations and international law is very promising in order to further elaborate on the makings and unmakings of normativities in global politics. These are omnipresent in global political processes. Studying them provides opportunities to zoom out and appreciate the multiplicities of global politics'.[59] In terms of underlying research philosophy and epistemological orientation, it stands in the tradition of interpretivism and constructivism, respectively.[60] Interpretivist research is founded on the belief that social realities are not singular or objective, but moulded by human experiences and social contexts. Consequently, processes of sense-making take precedence over endeavours of hypothesis testing.[61] Interpretivist inquiries tend to favour qualitative means and methods of data collection and evaluation.[62] Contrary to quantitative scholarly undertakings, which are slanted towards producing objective outcomes, generalisations, predictions, and cause-effect relationships by means

[59] Kornprobst (n 47) 321.

[60] John W Creswell, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (Fourth, SAGE Publications 2013).

[61] Anol Bhattacherjee, Interpretive Research (2019) ⟨http://perma.cc/3GSN-TKAL⟩ accessed 17 March 2019.

[62] Jerry Willis, *Foundations of Qualitative Research: Interpretive and Critical Approaches* (SAGE Publications 2007) ⟨http://perma.cc/95EZ-8N6K⟩; R Thomas, *Blending Qualitative & Quantitative Research Methods in Theses and Dissertations* (SAGE Publications 2003) ⟨http://perma.cc/U6BV-FKNB⟩.

of deductive reasoning, qualitative studies are preoccupied with (social) processes, contexts, interpretation, and understanding, generated through inductive reasoning.[63] It is worth noting that while the thesis has (predominantly) pursued inductive lines of reasoning, deductive elements often start to figure alongside inductive methods, and cannot categorically be excluded.

To comprehend social realities and elucidate phenomenological meaning, qualitative research designs often focus on small, purposefully selected samples (small-N research). 'The logic and power of purposeful sampling lies in selecting information-rich cases for study in depth. Information-rich cases are those from which one can learn a great deal about issues of central importance to the purpose of the research'.[64] To identify and contextualise the roles and contributions of non-state actors to global cybersecurity norm-making processes, this thesis draws on nine strategically selected, exploratory case studies, grouped into three stakeholder clusters.[65]

With regard to data collection, including the gathering of case materials, three main sources of input were used; (a) a large corpus of secondary academic literature and policy documents brought together by means of online desk research, (b) process observations, and (c) a compendium of semi-structured expert interviews with practitioners and scholars acquainted with norm construction projects pertaining to the digital domain.[66]

---

63 Kaya Yilmaz, 'Comparison of Quantitative and Qualitative Research Traditions: Epistemological, Theoretical, and Methodological Differences' (2013) 48(2) European Journal of Education 311 ⟨https://perma.cc/EAB3-A7EA⟩.

64 Michael Quinn Patton, *Qualitative Evaluation and Research Methods* (SAGE Publications 2002) ⟨https://perma.cc/WKY9-FZ95⟩ 230.

65 Case-oriented approaches allow for 'in-depth, multifaceted explorations of complex issues in their real-life settings', see Sarah Crowe and others, 'The Case Study Approach' (2011) 11(1) BMC Medical Research Methodology ⟨https://perma.cc/4JXD-EGCG⟩, 1. In addition to being valuable in historical description, they are useful in the development and refinement of theory, Jack S Levy, 'Qualitative Methods and Cross-Method Dialogue in Political Science' (2007) 40(2) Comparative Political Studies 196 ⟨https://perma.cc/QX6S-MGBT⟩. The criteria underlying the selection of cases were: policy relevance and comparability, analytical maturity, as well as availability of data and documentation.

66 Expert interviews were primarily employed as plausibility probes for textual and procedural observations, and to solidify findings.

The use of multiple sources of data, also referred to as data triangulation, allows researchers to obtain additional information, gain deeper phenomenological insights, and explore multiple realities.[67]

Data analysis was guided by thematic analysis. Thematic analysis denotes a well-established method used to rigorously and systematically analyse textual data.[68] It allows researchers to uncover, describe, and report themes within qualitative data, and elicit meaning and develop empirical knowledge.[69] The identification of categories or themes based on textual raw data entailed the following steps: (a) acquiring data familiarity, (b) generating initial codes, (c) searching for themes, (d) reviewing themes, (e) defining and naming themes, and (f) documenting themes (producing written output).[70] Data organisation, classification, and evaluation were supported by NVivo, a software package designed for computer-assisted qualitative data analysis.[71] The majority of data were iteratively analysed and coded by hand, however.

To facilitate the identification of non-state actor contributions to global cybersecurity norm formation processes and assess the effectiveness of their activities, this thesis has developed relevant analytical toolkits, including a contributions spectrum as well as an effectiveness assessment framework (please refer to Figure 3.1 and Figure 3.2 in *Chapter 3*, respectively). Conceptually, these tools help structure and categorise in qualitative terms the governance inputs of and roles taken on by non-state actors in cybersecurity norm formation ventures. By mapping and dissecting their contributions, these tools

---

67 Neil Salkind, *Encyclopedia of Research Design* (SAGE Publications 2010) ⟨https://perma.cc/U6BV-FKNB⟩; Crowe and others (n 65).

68 Elise Wach, Richard Ward, and Ruzica Jacimovic, *Learning about Qualitative Document Analysis* (techspace rep, August, Institute of Development Studies 2013) ⟨https://perma.cc/Y9M5-W6FQ⟩.

69 Glenn A Bowen, 'Document Analysis as a Qualitative Research Method' (2009) 9(2) Qualitative Research Journal 27 ⟨https://perma.cc/5MT5-W8MY⟩; Alan Bryman, *Social Research Methods* (5th edn, Oxford University Press 2015).

70 Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2006) 3(2) Qualitative Research in Psychology 77 ⟨https://perma.cc/9H67-93JB⟩.

71 QSR International, What is NVivo? (2017) ⟨https://perma.cc/7KDY-FLD5⟩.

assist in revealing new analytical categories and dimensions underlying/shaping global governance ventures. From the viewpoints of accountability and legitimacy, as well as public scrutiny it is important to know how and with which effects non-state actors influence global norm-making ventures, and to have relevant tools at hand to help conduct such analyses. What is more, effectiveness-oriented tools and investigations offer useful angles for examining the validity of prevalent theoretical assumptions, e.g. with regard to the identities of actors involved in global cybersecurity governance ventures.[72]

Although discussions about the development of global 'principles [to] enhance the security of ... information and telecommunications systems and ... to combat information terrorism and criminality' began to surface in the mid-1990s, the temporal focus of this study lies on the years following the non-consensus outcome of the 2016-17 UN GGE, which have seen increasing levels of non-state actor efforts pertaining to cybersecurity norms. It is important to note that the empirical and conceptual confines of this research project are inherently transitory and in constant flux. Such being the case, data reliability, validity, and generalisability have to be understood and evaluated within their discrete contexts of emergence. Notwithstanding the temporal and empirical limitations, this thesis is able to comment on the roles executed by non-state actors in global cybersecurity norm-making processes, and discuss their consequences for global accountability and legitimacy structures.

1.4 Thesis Structure

This dissertation is organised along eight chapters. Following this introductory chapter (*Chapter 1*), which has acquainted readers with the topic under investigation, outlined the broader context this study is situated in, and introduced the main research question, *Chapter 2* summarises the conceptual lines of thinking underpinning this study. It

[72] Ulbert (n 50).

reviews relevant secondary bodies of work in the areas of international relations and international law pertaining to cybersecurity, and clarifies terminologies used. Based on the reviews performed, it calls for more empirically-grounded frames of reference pertaining to the types of agency executed and contributions made by non-state actors in/to global cybersecurity governance processes.

Chapter 3, Methodology, Data, and Analytical Tools introduces the ontological and epistemological premises of this study and comments on the means and methods of data collection and analysis employed. It specifies the sampling tactics used to select relevant case studies, and presents the structural skeleton underlying each of the empirical examples.[73] It also familiarises readers with the analytical tools developed to conduct the planned investigations. The chapter ends with remarks on the limitations of the data gathering and evaluation strategies used, and puts them into perspective.

Chapters 4, *5*, and *6*, review and examine different non-state actor endeavours pertaining to the construction of norms of responsible behaviour in cyberspace. Grouped into three stakeholder clusters, (a) civil society and academia, (b) corporate actors, and (c) expert communities, the empirical examples selected for analysis include the following entities: (a) Global Partners Digital, (b) the second International Group of Experts, (c) the Hague Program for Cyber Norms, (d) Microsoft, (e) Siemens, (f) Kaspersky Lab, (g) the Global Commission on the Stability of Cyberspace, (h) the Forum of Incident Response and Security Teams (FIRST), and (i) Carnegie Endowment for International Peace. The case studies evidence that 'the widening gap between the need for normative clarity in cyberspace, on the one hand, and the possibilities of achieving consensus or agreement around norms, on the other', has afforded considerable influence to actors which traditionally have been at the

[73] Each case study is structured along the following sections: background, mandate and goals, activities, role profiles, effectiveness review, précis.

periphery of global norm-making projects.[74] Broadening existing theoretical models centred on advocacy and lobbying, and advancing empirically more informed and varied conceptualisations of the parts played by non-state actors in cybersecurity norm creation projects, this dissertation argues that their roles can be systematised along the following profiles: (a) knowledge brokers, (b) awareness raisers, (c) norm leaders and cooperation incubators, (d) diplomatic change agents, (e) discussion feeders and gap fillers, (f) implementation assistants and capacity builders, and (g) custom shapers.

Chapter 7, Implications and Challenges, reviews the findings of *Chapters 4*, *5*, and *6*, and comments on their wider implications for global cybersecurity governance arrangements. The contributions of non-state actors to cybersecurity norm-making processes raise important legitimacy and accountability questions. They also raise questions about sites of influence and suitable forms of interaction between state and non-state actors. This chapter purports that in the context of cybersecurity, '[power] to set standards is dispersed amongst and between actors, ... [operating] on a continuum between state and non-state spheres'.[75] Rather than signalling a linear decrease or increase of norm-making capacity on either the parts of sovereign entities or non-state actors, the multiplication of norm-making protagonists first and foremost implies that underlying structures of agency are shifting, and new forms of regulation and sites of authority are emerging.

Chapter 8, titled Conclusion, summarises the main contributions of this thesis and highlights impending questions related to global cybersecurity norm cultivation projects. It contends that in order to move norm construction efforts forward, and find palpable solutions to problems of cyberinsecurity, more refined understandings of and

---

74 Global Commission on the Stability of Cyberspace, *Briefings from the Research Advisory Group* (techspace rep, November, 2017) ⟨https://perma.cc/HYQ4-GXSP⟩ 51.

75 Anne Peters, Lucy Koechlin, and Gretta Fenner Zinkernagel, 'Non-State Actors as Standard Setters: Framing the Issue in an Interdisciplinary Fashion' in Anne Peters and others (eds), *Non-State Actors as Standard Setters* (Cambridge University Press 2009) ⟨https://perma.cc/U5J2-8B3J⟩ 23.

appreciation for the roles of non-state actors are crucial, both from theoretical as well as practical viewpoints. As governmental endeavours continue to be 'overshadowed or undermined by conflicting national interests, reciprocal distrust, and/or geopolitical disputes that spill over from other issue areas', it is especially important for non-state actors to continue their efforts.[76] Although not endowed with formal law-making capacities under positivist notions of international law and international relations, the work of non-state actors is exceptionally important in terms of lining out and shaping the boundaries of responsible behaviour in cyberspace. Furthermore, the norm-building activities of non-state actors point to a need for more collaborative governance setups, in which the former participate in joint steering efforts and share responsibilities with sovereign authorities. *Chapter 8* concludes with brief comments on possible trajectories for future research.

---

[76] Tanczer, Brass, and Carr (n 34); Liis Vihul, The Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) ⟨https://perma.cc/P4FM-HQHP⟩ accessed 23 February 2018.

Despite states' traditional dominance over all questions related to international peace and security, [their] role within the overall cyberspace ecosystem is limited. After all, the internet is governed by a complex ecosystem of stakeholders, each with its own set of standards, norms, rules and processes. Governments alone cannot decide on all aspects of cyberspace – a space in which civil society writes much of the key code and the private sector owns nearly all the digital and physical assets.

— Marina Kaljurand, *Editorial for the Munich Cyber Security Conference (2018)*

.

2

Literatures and Concepts

Contents

This chapter introduces and summarises central concepts and tenets underlying the inquiry at hand. It clarifies terminologies employed, appraises theoretical bodies of work pertaining to cybersecurity, and reviews leading analytical standpoints in the areas of international relations and international law. It seeks to offer contextual baselines and insights for the subsequent discussions concerning the complexities of non-state actor-driven cybersecurity norm formation ventures.

Following terminological explications concerning cyberspace and cybersecurity, as well as summaries of influential scholarly publications pertaining to cybersecurity, this chapter proceeds with an overview of leading norms-related theories and approaches. It then continues with an outline of key conceptualisations of non-state actors across international relations and international law literatures, before recapitulating the main

theoretical insights acquired.[77] The chapter argues that although recognised as entities under international law and international relations, in the context of cybersecurity, non-state actors have received little extensive scholarly treatment apropos their contributions to global regulatory schemes and merit further investigation.

Before delving into conceptual discussions, it is worth recalling that the scientific determinants at the heart of this analysis look back on a history of little more than fifty years.[78] Much of what is referred to as cyberspace, both in common and scholarly parlance, is rooted in the workings of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and relevant extensions. Research on TCP/IP began in 1973, with the resulting protocols seeing widespread adoption ten years later.[79] The early 1990s, marked by the advent of the World Wide Web, rang in the percolation of internet-based technologies into wider society. Vast numbers of cyber-dependent products and services have developed since.[80] Today, computer systems and networks have acquired the status of *General Purpose Technologies*, and underpin critical systems of socio-political and economic importance.[81]

---

77 Noortmann and Ryngaert (n 38); Joseph SJr Nye and John D Donahue, *Governance in a Globalizing World* (Brookings Institution Press 2000); John Gerard Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations' (1993) 47(1) International Organization 139 ⟨https://perma.cc/DQR5-ZBTB⟩; Bas Arts, Math Noortmann, and Bob Reinalda, *Non-State Actors in International Relations* (Ashgate 2001); Andrea Bianchi, 'The Fight for Inclusion: Non-State Actors and International Law' in *From Bilateralism to Community Interest* (Oxford University Press 2011) ⟨https://perma.cc/R285-SK6V⟩.

78 In 1969, the Advanced Research Projects Agency (ARPA), under the aegis of the United States Department of Defence, instituted a four-node network, called ARPANET (Advanced Research Projects Agency Network), which connected mainframes at the University of California Los Angeles, Stanford University, the University of California Santa Barbara, and the University of Utah. ARPANET served as the progenitor of cyberspace as it is known today, see Shackelford (n 35).

79 The migration of ARPANET from the Network Control Protocol to the Transmission Control Protocol/Internet Protocol (TCP/IP) on 1st January 1983, marked the official flag day for what is now considered to constitute modern cyberspace, see Leiner and others (n 35); Joseph SJr Nye, 'Cyber Power' [2010] (May) Belfer Center for Science and International Affairs 1 ⟨https://perma.cc/GHB4-63ED⟩.

80 John Naughton, 'The Evolution of the Internet: From Military Experiment to General Purpose Technology' (2016) 1(1) Journal of Cyber Policy 5 ⟨https://perma.cc/E92M-XEJZ⟩.

81 General Purpose Technologies have the capacity to exert considerable influence on and alter

2.1 Cyberspace and Cybersecurity

Cyberspace represents the most elemental concept underlying this inquiry.[82] It lays out the context within which norm formation projects are construed and analysed.[83] Even though cyberspace has become deeply embedded in everyday life, divergent understandings apropos its constitutive elements as well as terminological ambiguity appear to persist. From the standpoints of theory and practice, the absence of definitional consistency is of relevance insofar as it substantially increases the chances for theoretical contradiction and conceptual misrepresentation.[84]

While this chapter comments on some of the conceptual quarrels relating to theoretical constructs such as cyberspace and cybersecurity, its goal is not to engage in extensive reviews of these definitional struggles but to establish a common point of departure for the succeeding chapters.[85]

---

established socio-economic structures. They typically exhibit three key characteristics. They are (a) widely employed, (b) susceptible to continuous improvement and transformation, and (c) of innovation-enabling nature, see Timothy Bresnahan, 'General Purpose Technologies' in Bronwyn H Hall and Nathan Rosenberg (eds), *Handbook of the Economics of Innovation* (Elsevier Science 2010).

82 Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (2013) 38(2) International Security 7 ⟨https://perma.cc/2CSB-58RZ⟩.

83 Etymologically, cyberspace is a composite term of the noun *space* and the derivation of the ancient Greek word κυβερνήτης (kybernētēs), which translates as captain, governor, guide, or steersman. In popular culture, the term cyberspace started to gain traction in the early 1980s when it began to figure in literary works, including William Gibson's widely acclaimed 1984 science fiction novel *Neuromancer*, see William Gibson, *Neuromancer* (Berkley Publishing Group 1984).

84 With regard to global norm creation endeavours, for example, arriving at widely-accepted rules of the road for cyberspace 'becomes more difficult, although not impossible, if the scope of what to be governed is fundamentally disputed', James Shires and Max Smeets, 'What Do We Talk About When We Talk About Cyber?' [2016] SSRN Electronic Journal ⟨https://perma.cc/UD9S-D645⟩, 3.

85 Comprehensive collections of cybersecurity-related terms as well as definitional explications can be found elsewhere, see, for example, NATO Cooperative Cyber Defence Centre of Excellence, Strategy and Governance (2019) ⟨https://perma.cc/LQ65-3TZN⟩ accessed 11 April 2019; Tim Maurer and Robert Morgus, *Compilation of Existing Cybersecurity and Information Security Related Definitions* (techspace rep, New America 2014) ⟨https://perma.cc/PWD7-HKLY⟩; Tim Maurer and Robert Morgus, 'Cybersecurity' and Why Definitions Are Risky (2014) ⟨https://perma.cc/ZC3R-4P34⟩ accessed 11 April 2019; Richard L Kissel, *Glossary of Key Information*

2.1.1 Traversing Conceptual Muddles

Cyberspace is often equated with the World Wide Web, but the two are not identical. Cyberspace can be thought of as a network of networks, including both open and closed systems. The World Wide Web on the other hand denotes an information space with information resources identified by Uniform Resource Identifiers, which are accessible via cyberspace.[86] For the purposes of this thesis, the terms *cyberspace*, *virtual realm*, and *digital domain* are used interchangeably. The number of definitional accounts pertaining to cyberspace is bewilderingly large, ranging from technical to socio-political and economic descriptions.[87]

To illustrate, Kuehl has defined cyberspace as a

> global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[88]

His understanding of cyberspace makes partial reference to US military doctrine, which has considered cyberspace to represent the fifth domain of warfare, co-equal to the four traditional domains of land, sea, air, and space.[89]

Security Terms (techspace rep, National Institute of Standards and Technology 2013) ⟨https://perma.cc/2WPU-LMU3⟩; Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' [2013] 5th International Conference on Cyber Conflict 1 ⟨https://perma.cc/6Q2Z-Y7J2⟩.

86 World Wide Web Consortium, World Wide Web (2019) ⟨https://perma.cc/9FAZ-SCGL⟩ accessed 31 March 2019.

87 Franklin D Kramer, 'Cyberpower and National Security: Policy Recommendations for a Strategic Framework' in Franklin D Kramer, Stuart H Starr, and Larry K Wentz (eds), *Cyberpower and National Security* (National Defense University Series, Potomac Books Inc 2009).

88 Daniel T Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem' in Franklin D Kramer, Stuart H Starr, and Larry K Wentz (eds), *Cyberpower and National Security* (Potomac Books Inc 2009).

89 The United States Department of Defense has defined cyberspace as 'a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers', US Department of Defense, *DoD Dictionary of Military and Associated Terms* (techspace rep, 2019) ⟨https://perma.cc/P9NS-NJWW⟩ 59.

In contrast to Kuehl's technical definition of cyberspace, the International Organisation for Standardisation (ISO) has construed cyberspace as a 'complex environment resulting from the interaction of people, software and services on the internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks'.[90] Choucri and Clark have advocated for a layered conception of cyberspace.[91] In their view, cyberspace consists of four distinct, yet interdependent layers: (a) a physical layer, comprising tangible infrastructure, including, wires and computer boxes; (b) a logical layer, consisting of protocols, the Domain Name System (DNS), and software; (c) an information layer, encompassing text, photos, videos, and other user-generated information; (d) and a user layer, involving 'people and constituencies who shape the cyberexperience and the nature of cyberspace itself, by communicating, working with information, making decisions and carrying out plans'.[92]

While different in scope and ontological orientation, the approaches outlined above share several consistent threads, including references to infrastructures, interconnected networks, as well as information systems.[93] Taking these features into account, and ascribing relevance to socio-economic patterns of dependence and influence, this thesis considers cyberspace to denote 'all computer systems and networks in existence, including air-gapped systems'.[94] In addition to the internet which consists of all interconnected computing devices, including the World Wide Web, cyberspace also

---

90 International Organisation for Standardisation, ISO/IEC 27032:2012 (2012) ⟨https://perma.cc/42LC-QM33⟩ accessed 31 March 2019.

91 Choucri and Clark (n 14).

92 ibid 2-3. The broad range of meanings attached to cyberspace has led some scholars to think of it as an *essentially contested concept*, see Walter Bryce Gallie, 'Essentially Contested Concepts' (1956) 56 Proceedings of the Aristotelian Society 167 ⟨https://perma.cc/TAX3-PDR3⟩; Shires and Smeets (n 84). According to Gallie, essentially contested concepts denote concepts which involve endless discussions and are so value-laden that no amount of evidence can bring to the fore correct or 'proper uses on the part of their users', Gallie (n 92); David A Baldwin, *The Concept of Security* (vol 23, 1997) ⟨https://perma.cc/6GNA-9N69⟩ 169.

93 Kuehl (n 88).

94 Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82) 17.

comprises the entirety of secluded systems, which are not logically connected to the internet or the World Wide Web.

As Kello has pertinently noted,

> not all threats propagated through the web can transmit via the internet, and those that are transmissible cannot use the internet to breach the cyberarchipelago [(i.e., all other computer systems that exist in theoretical seclusion)]. On these terms, there are two basic kinds of targets: (a) remote-access and (b) closed-access.[95]

This thesis recognises both the physical and less physical, socio-informational characteristics of cyberspace, as well as the susceptibility of ICTs to human interaction and modification.

The proliferation of cyberthreats and incidents involving network infrastructures has led to shifts in the perception of the virtual realm. At the outset a science and engineering driven project, cyberspace has become (portrayed as) an area of strategic concern, a domain of power execution, and a zone of conflict and ill-doing.[96] Over the years, cyberspace has evolved from a matter of low politics to a matter of high politics, challenging and subverting traditional notions of leverage and influence, borders and boundaries, as well as modes of transaction and interconnection.[97]

In light of burgeoning levels of economic, political, and cultural dependence, the protection and securing of computer systems and networks as well as reliant

---

95 Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82) 17-18. Examples of open network exploitations include the German parliament email hack (2019) as well as the Norsk Hydro ransomware attack (2019), see BBC News, German Politicians Targeted in Mass Data Attack (2019) ⟨https://perma.cc/K7MQ-SAC9⟩ accessed 11 April 2019; Hans-Edzard Busemann and Tassilo Hummel, German Politicians' Data Published Online in Massive Breach (2019) ⟨https://perma.cc/E72S-NJQZ⟩ accessed 2 April 2019; Gwladys Fouche and Terje Solsvik, Aluminum Maker Hydro Battles to Contain Ransomware Attack (2019) ⟨https://perma.cc/R264-TV2U⟩ accessed 2 April 2019. The cyberoperation Olympic Games (2010), better known under the name Stuxnet, is often cited as an example of a closed network attack, see Ralph Langner, *To Kill a Centrifuge* (techspace rep, The Langner Group 2013) ⟨https://perma.cc/J3BC-6UN7⟩.

96 Jacqueline Eggenschwiler, 'Accountability Challenges Confronting Cyberspace Governance' (2017) 6(3) Internet Policy Review 1 ⟨https://perma.cc/3KT6-SHGP⟩.

97 Choucri and Clark (n 14).

infrastructures have become key concerns for public and private entities.[98] To illustrate, according to insights gathered by global research and consultancy firm Gartner, worldwide cybersecurity spending, both public and private, was forecast to exceed USD 124 billion in 2019, representing an 8.7% increase compared to 2018.[99] The forecast relied on responses from 480 survey participants from eight nations, including Australia, Canada, France, Germany, India, Singapore, the United Kingdom, and the United States.[100]

In terms of conceptual coherence, cybersecurity struggles with similar definitional ambiguities as cyberspace. However, the challenges associated with conceptualising security issues antedate interconnected ICTs and network infrastructures.[101] Indeed, questions concerning the constitutive elements of security have been at the centre of security studies, a sub-field of international relations research, for many years. Wolfers, for example, in his seminal essay entitled *'National Security' as an Ambiguous Symbol* argued that 'the term *security* covers a range of goals so wide that highly divergent policies can be interpreted as policies of security'.[102] Citing and building on Wolfers' conceptual work, Baldwin too, maintained that security is in need of more explication.[103] Viewing nation states as the relevant referent objects, and seeking to

---

98 Kremer and Müller (n 3); Mark Raymond and Laura DeNardis, 'Multistakeholderism: Anatomy of an Inchoate Global Institution' (2015) 7(3) International Theory 572 ⟨https://perma.cc/L5AK-ZTP2⟩.

99 Susan Moore and Emma Keen, Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 (2018) ⟨https://perma.cc/8W6J-FWH8⟩ accessed 3 April 2019.

100 Roger Aitken, Global Information Security Spending to Exceed $124B in 2019, Privacy Concerns Driving Demand (2018) ⟨http://perma.cc/Q9ER-K8SJ⟩ accessed 3 April 2019. The US government alone dedicated USD 15 billion for cybersecurity-related activities as part of the President's budget for fiscal year 2019, denoting a 4.1% increase from the estimate for fiscal year 2018, see Office of Management and Budget, *An American Budget, Fiscal Year 2019* (techspace rep, 2018) ⟨https://perma.cc/4EJA-9N49⟩.

101 Josephine Wolff, 'What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates' (2016) 5(3) Internet Policy Review 1 ⟨https://perma.cc/6TC6-W33F⟩.

102 Arnold Wolfers, 'National Security as an Ambiguous Symbol' (1952) 67(4) Political Science Quarterly 481 ⟨https://perma.cc/E7A3-BQ28⟩, 484.

103 Baldwin (n 92).

provide conceptual starting points, Wolfers held that 'security, in an objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked'.[104]

The conceptualisation of security as the absence of threats has also reverberated with computer scientists.[105] Employing different referent objects, i.e. systems and networks, computer scientists have delineated security as the absence of threats to the confidentiality, integrity, and availability of systems and data.[106] The so-called CIA triad has been at the heart of information security definitions for many years. As systems and network environments have grown and become ever more complex, the three security objectives have come under increasing scrutiny, however. Among other things, critics have argued that the CIA triad fails to sufficiently address emerging information security challenges, and requires adjustments and corrections to include aspects such as privacy, trust, non-repudiation, or authenticity.[107] Despite numerous appeals for theoretical extensions, confidentiality, integrity, and availability have retained important conceptual validity, even beyond techno-computational confines. Several nation states

---

104 Wolfers (n 102) 485.

105 Rather than making reference to cybersecurity, researchers in the filed of computer science have traditionally conceptualised security in terms of information and network security. Information security refers to the 'protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information', Michael E Whitman and others, *Guide to Network Security* (Cengage Learning 2012) 3. Network as well as computer security are considered subsets of information security.

106 Peter Warren Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014); Sean Brooks and others, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (techspace rep, National Institute of Standards and Technology 2017) ⟨https://perma.cc/DH89-EAAL⟩. Confidentiality refers to the prevention of unauthorised access to or disclosure of information. Conceptually, it is closely connected to notions of privacy and authorisation. Integrity entails the preservation of accuracy and completeness and the prevention of destruction or modification of data and systems respectively. Availability involves the assurance of timely and reliable access to systems and data, see Gurpreet Dhillon and James Backhouse, 'Technical Opinion: Information System Security Management in the New Millennium' (2000) 43(7) Communications of the ACM 125 ⟨https://perma.cc/2U5C-KJEE⟩; Shari Lawrence Pfleeger and Charles P Pfleeger, *Security in Computing, Third Edition* (3rd, Prentice Hall 2002); Bowen (n 69); Kissel (n 85).

107 Donn B Parker, *Fighting Computer Crime: A New Framework for Protecting Information* (J Wiley 1998); Whitman and others (n 105); Michael E Whitman and Herbert J Mattord, *Management of Information Security* (Cengage Learning 2017).

as well as international organisations have made reference to the three security objectives as stipulated by computer scientists in their definitions of cybersecurity.

The European Commission, for example, has defined cybersecurity as

> the safeguards and actions that can be used to protect the cyberdomain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.[108]

The International Telecommunications Union (ITU) has advanced an even more comprehensive definition of cybersecurity. As per recommendation *ITU-T X.1205*,

> [c]ybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality.[109]

Apart from these primarily technology- and data-oriented understandings of cybersecurity, there have also been more doctrinal approaches, focusing on issues of national security and premeditated interests. Kello, for example, has argued that while cybersecurity relates to the absence of unauthorised interference with digital resources as well as their uninhibited functioning, it also comprises 'the safety and survivability of functions operating beyond cyberspace but still reliant on a computer

---

[108] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (2013) ⟨https://perma.cc/27F8-5W7J⟩ 3.

[109] International Telecommunications Union, Definition of Cybersecurity (2008) ⟨https://perma.cc/88DW-9MYA⟩ accessed 8 April 2019, 2.

host, to which they are linked at the logical or information layer'.[110] Underscoring the strategic importance of cyberspace and the practices related to its safekeeping, the Government of the United Kingdom, for instance, has maintained that cybersecurity encompasses both the protection and defence of UK interests in the virtual realm and 'also the pursuit of wider UK security policy through exploitation of the many opportunities that cyberspace offers'.[111]

China and Russia, too have given priority to strategic considerations in their definitions of cybersecurity. Beijing and Moscow have lobbied for exclusive control over information distributed within their respective sovereign confines.[112] *Information security* rather than cybersecurity has served as conceptual roof under which measures such as internet censorship or government-based controls of information flows have been subsumed.[113] Contrary to Euro-Atlantic considerations of cybersecurity, Sino-Russian conceptions of information security extend beyond networked resources and ICTs, and include human information processing (cognitive spaces) as well as information systems.[114] As will be evidenced later on, these alternative interpretations among

---

110 Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82) 18.

111 Cabinet Office, *Cyber Security Strategy of the United Kingdom* (techspace rep, June, 2009) ⟨https://perma.cc/SE9M-QTPW⟩ 9.

112 Andrew Radin and Clinton Reach, *Russian Views of the International Order* (techspace rep, RAND Corporation 2017) ⟨https://perma.cc/9QSX-NRAR⟩.

113 Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82); Yuan Yang, The Great Firewall of China: Web of Control (2019) ⟨https://perma.cc/A4VY-AS8F⟩ accessed 13 April 2019. The Kremlin's ideas about information security are evident in its 2013 *Concept of the Foreign Policy of the Russian Federation*, which stated that Russia 'will take necessary measures to ensure national and international information security, prevent political, economic and social threats to the state's security that emerge in information space in order to combat terrorism and other criminal threats in the area of application of information and communication technologies, [and] prevent them from being used for military and political purposes that run counter to international law, including actions aimed at interference in the internal affairs and constituting a threat to international peace, security and stability', Ministry of Foreign Affairs of the Russian Federation, Concept of the Foreign Policy of the Russian Federation (Unofficial Translation) (2013) ⟨https://perma.cc/3S6D-9AS4⟩ accessed 13 April 2019.

114 Timothy L Thomas, *Information Security Thinking: A Comparison Of US. Russian, and Chinese Concepts* (techspace rep, Foreign Military Studies Office 2001) ⟨https://perma.cc/X642-856Y⟩. 'According to official Chinese sources, the internet has the capability to manipulate information, the truth, and the moral-psychological state of Chinese citizens', ibid 3.

Eastern and Western proponents and their respective allies have repeatedly undermined efforts to establish international regimes of rules and norms of responsible behaviour for the virtual realm.[115]

Acknowledging that the consequences of cyberinsecurity propagate beyond technical confines, and taking into account the definitional struggles surrounding it, while paying due regard to its underlying technical determinants, this thesis understands cybersecurity as a

> multifaceted set of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorised access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information.[116]

This dissertation recognises that absolute security is an ideal state and impossible to attain. Security involves the management of trade-offs. This thesis also takes note of and underscores the relational aspects of cybersecurity. Cybersecurity practices are determined by a wide variety of stakeholders that employ different threat perceptions (political, private, societal, and corporate notions of security) to charge and discharge different referent actors/audiences.[117]

---

115 Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82).

116 Myriam Dunn Cavelty, 'Cyber-Security and Private Actors' in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies* (Routledge 2015) ⟨https://perma.cc/Y47N-DWUE⟩ 89.

117 ibid. Balzacq and Dunn Cavelty aptly stated that '[c]ybersecurity is co-produced by every private computer user, by computer security specialists in the server rooms of this world, by programmers, by Chief Information Officers (CIOs) or Chief Executive Officers (CEOs) deciding on cybersecurity investments, by security consultants, by [cyberforensic scientists], by regulatory bodies and standardisation organisations, [as well as] ... by politicians and other government officials that interpret digital events and (re)act to them in the form of verbalised expectations and fears or ultimately, policies', Thierry Balzacq and Myriam Dunn Cavelty, 'A Theory of Actor-Network for Cyber-Security' (2016) 1(2) European Journal of International Security 176 ⟨https://perma.cc/5JTM-RMYC⟩, 180.

2.1.2 Conceptualising Security Issues

Issues pertaining to the security of the virtual realm started to receive scholarly attention in the areas of international relations and international law in the mid-1990s. Prior to the mid-1990s, the government-sponsored network research project (ARPANET) that became the internet, lacked the critical mass and social uptake to incite scholarly debates across disciplines other than electrical engineering or computer science. TCP/IP-based networks were 'not yet geographically or economically vital', and perceptions of insecurity not yet imminent enough to stimulate social scientific and legal inquiries.[118] As networked machines began to spread, and security threats as well as levels of political, economic, and social dependence began to increase and become more palpable, however, scholars in the fields of international relations and international law started to study the implications of networked infrastructures on principles of global ordering and governance, as well as their effects on central concepts such as power, control, sovereignty, deterrence, war, and defence.[119]

Early pioneers in the discipline of international relations were primarily concerned with questions connected to how ICTs alter 'the way advanced societies conduct war and make peace', and militarise cyberspace, respectively, while initial legal research concentrated on issues related to the regulability of the digital realm.[120] The decade

---

[118] Shackelford (n 35) 28.

[119] Among others, authors including Choucri, Demchak and Dombrowski, as well as Kello have actively called on the broader international relations community to address questions pertaining to cybersecurity, and develop appropriate concepts to analyse related phenomena, see Choucri and Clark (n 14); Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82); Chris Demchak and Peter Dombrowski, 'Cyber Westphalia: Asserting State Prerogatives in Cyberspace' [2014] Georgetown Journal of International Affairs 29 ⟨https://perma.cc/79C5-HA6T⟩. Kello, for instance, has noted that '[t]he growth of technological ability is rapidly outpacing the design of concepts to interpret it', and has provided useful insights for conceptual refinements, see Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press 2017) ⟨https://perma.cc/T2T6-ZFHD⟩ 7.

[120] James Der Derian, 'The Question of Information Technology in International Relations' (2003) 32(3) Millennium: Journal of International Studies 441 ⟨https://perma.cc/7QVR-MXMP⟩, 447. See also Ronald J Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation

before the turn of the 21st century was dominated by strong notions of post-territoriality. Cyberspace was seen to be at odds with traditional concepts of organisation and control.[121] It was widely held that the borderless and non-proprietary nature of the digital domain, its decentred and distributed structure fundamentally challenge key tenets of sovereign authority.

In their seminal paper titled *Law and Borders: The Rise of Law in Cyberspace*, Johnson and Post, for example, contended that cyberspace severely undermines the nexus between physical location and regulatory reach. Specifically, they argued that the rise of global, interconnected ICTs

> is destroying the link between geographical location and: the power of local governments to assert control over online behaviour; the effects of online behaviour on individuals or things; the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and the ability of physical location to give notice of which sets of rules apply.[122]

Consequently, they believed the application and enforcement of geographically-inspired laws to be ineffective in the context of cyberspace. They maintained that the digital realm requires its own set of rules, distinct from territorially-centred practices of nation states. These claims were later challenged by scholars, including Joel Reidenberg

---

of Cyberspace' (2003) 32(3) Millennium: Journal of International Studies 501 ⟨https://perma.cc/MWB7-W3UU⟩; David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367 ⟨https://perma.cc/PK8M-Z4H2⟩; Frank H Easterbrook, 'Cyberspace and the Law of the Horse' [1996] (1) University of Chicago Legal Forum 207 ⟨https://perma.cc/3TMT-4AZ4⟩; Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76(3) Texas Law Review 553 ⟨https://perma.cc/WPX4-6BBE⟩; Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books 2006).

121 This line of thinking came to be referred to as cyberlibertarianism. Grounded in right-wing libertarian ideals, such as radical individualism, equality before the law, freedom of speech and expression, self-ownership, and sovereign non-intervention, scholars and practitioners adhering to this school of thought considered cyberspace to fall outside the remit of centralised state oversight. John Perry Barlow, founding member of the Electronic Frontier Foundation (EFF) and author of the *Declaration of the Independence of Cyberspace*, is frequently cited as one of the key proponents of the cyberlibertarian movement, see John P Barlow, A Declaration of the Independence of Cyberspace (1996) ⟨https://perma.cc/DRJ9-WEGT⟩ accessed 19 November 2019.

122 Johnson and Post (n 120) 1370.

as well as Lawrence Lessig, who argued that the virtual realm was in fact rather strictly regulated by its architectural features and technological capabilities, and did not escape the regulatory grip of sovereign actors.[123]

Questions related to how cyberspace shapes power in global affairs also took centre stage in political oeuvres, including in Joseph Nye's book *The Future of Power: Its Changing Nature and Use in the Twenty-First Century.* In his manuscript, Nye maintained that cybertransformations are 'changing the nature of power and increasing its diffusion' from large, resource-heavy states to smaller governments and non-state actors.[124] Following similar lines of argument, Klimburg highlighted three different dimensions of cyberpower, and discussed the interactions between state and non-state entities in the virtual realm, as well as the use of proxy-actors to project influence.[125]

Thematically connected to considerations of power projections, scholars including Hansen and Nissenbaum, Dunn Cavelty, as well as Deibert and Rohozinski analysed how matters related to cyberspace had become portrayed as high-level security issues.[126]

---

123 Reidenberg (n 120); Lessig (n 120). Reidenberg and Lessig were considered key proponents of cyberpaternalism. Argumentatively situated within a period of increasing commercialisation, driven in large part by the arrival of the World Wide Web, cyberpaternalists did not believe that the digital realm constituted an environment outside the scope of territorially-based steering, or that nation states were devoid of regulatory capacity, or that the different dimensions of internetworking could only be governed meaningfully by emergent regulatory structures produced by distributed collective action. And indeed, today's realities seem far removed from the non-interventionist regulatory doctrines advanced by cyberlibertarian thinkers. Cyberpaternalist credos and manifestations of sovereign control appear to 'have consigned cyberlibertarianism to the pages of history books', see Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2013) 81. Far from being unregulable, cyberspace has become the subject of excessive global public and private ordering efforts.

124 Joseph SJr Nye, *The Future of Power: Its Changing Nature and Use in the Twenty-First Century* (PublicAffairs 2011) 114.

125 Alexander Klimburg, 'Mobilising Cyber Power' (2011) 53(1) Survival 41 ⟨https://perma.cc/8ZNN-AEBQ⟩. The three dimensions of cyberpower referenced by Klimburg include: (a) the coordination of operational and policy aspects across national structures, (b) the consistency of policy through international alliances and legal frameworks, as well as (c) the support of non-state cyberactors, see ibid 43.

126 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge 2008); Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School' (2009) 53(4) International Studies Quarterly 1155 ⟨https://perma.cc/MQ5B-5WMG⟩; Ronald J Deibert and Rafal Rohozinski, 'Risking Security: Policies and Paradoxes

Employing securitisation concepts, Dunn Cavelty, for example, traced the political processes behind the construction of cyberthreats as key security concerns in the US from the 1980s to the early 2000s.[127] Her analysis focused on uncovering threat frames and interpretative schematics used by public actors to place issues pertaining to the virtual realm onto security agendas and into political spheres (threat politics).[128] According to Dunn Cavelty, one of the main reasons for why cyberthreats had received increasing amounts of attention, 'is the fact that in the process of threat politics, US officials have convincingly argued that they [threaten] the very fabric of modern societies'.[129] 'The urgency of fighting cyberthreats', Dunn Cavelty argued, 'was established by linking them to the concept of critical infrastructures'.[130] Deibert and Rohozinski, in their article *Risking Security: Policies and Paradoxes of Cyberspace Security*, provided a detailed account of the implications of securitisation processes on internet freedom. They argued that while governments 'seek policy coordination and regulations so as to make cyberspace ... more secure, safe, and predictable', at the same time, they respond to risks through cyberspace (as opposed to risks to cyberspace) with paradoxical measures that limit the uninhibited use of ICTs by networked political or social actors,

---

of Cyberspace Security' (2010) 4(1) International Political Sociology 15 ⟨https://perma.cc/P58M-ETF7⟩.

127 Theoretically underpinned by constructivist insights, securitisation approaches hold that issues (political or non-political) become quintessential security concerns as a result of deliberate framing efforts (labelling issues as *menacing, alarming, or threatening)* by securitising actors who boast enough social and institutional influence to move and remove issues onto/from relevant security agendas. Hence, security issues do not exist a priori but are the products of deliberate, socially constructed, contextual speech acts, see Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (n 126); Clara Eroukhmanoff, 'Securitisation Theory' in Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug (eds), *International Relations Theory* (E-International Relations Publishing 2017) ⟨https://perma.cc/QE6U-CLVC⟩. This in turn implies that issues are made security concerns not necessarily as a consequence of the presence of real-life threats but as a result of strategic assessments and power considerations and relevant discursive dominance, see Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (n 126); Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Lynne Rienner 1998).

128 Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (n 126).

129 Ibid 138.

130 Ibid 141.

e.g. through content filtering, intimidation and self-censorship as a result of pervasive surveillance efforts, or disconnection of critical infrastructures.[131]

The discovery of the Stuxnet malware in June 2010 gave rise to a soaring number of publications on cyberwar.[132] Considered to be the first cyberattack to have crossed the use-of-force threshold (with targeted kinetic effects), the detection of the Stuxnet operation is often cited as a 'turning point in the history of cybersecurity'.[133] Post-2010, political as well as legal scholars started addressing a wide variety of questions related to cyberwar, ranging from what it is, to whether it will take place, to how it is to be regulated.[134]

One of the first accounts published in the early 2010s, aiming to shed more light on

---

131 Deibert and Rohozinski (n 126) 17.

132 The Stuxnet malware, identified by Belarusian antivirus company VirusBlokAda, formed part of a more extensive, classified programme called *Operation Olympic Games*, which is said to have been launched under the George W. Bush administration and later continued under the Obama administration, see Josh Fruhlinger, What Is Stuxnet, Who Created It and How Does It Work? (2017) ⟨https://perma.cc/4FHJ-S5P9⟩ accessed 4 May 2019. Widely acknowledged to have been the product of US and Israeli intelligence agencies, the Stuxnet malware was crafted to halt Iran's uranium enrichment efforts by damaging centrifuge rotors at the Natanz nuclear facility, see Ralph Langner, 'Stuxnet: Dissecting a Cyberwarfare Weapon' (2011) 9(3) IEEE Security & Privacy Magazine 49 ⟨https://perma.cc/EVQ6-AC7Y⟩; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishers 2014). Believed to have entailed two different attack routines (over-pressurisation and over-acceleration), the attack sequence which sought to infiltrate the logical environment of the Siemens S7-315 programmable logic controller (PLC) has received most expert attention to date. The S7-315-related attack sequence was designed to inject 'malicious code into the PLC to alter the behaviour of IR-1 centrifuge cascades controlled by it', and render the gas centrifuges useless by negatively affecting their enrichment efficiency, see Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (n 82) 19. For more detailed information about the attributes of the malicious software, as well as the attack and propagation mechanisms employed, please refer to Langner, *To Kill a Centrifuge* (n 95), who has provided one of the most pervasive accounts on the malware. Zetter (n 132) is also a useful resource for more information on the Stuxnet worm.

133 Langner, *To Kill a Centrifuge* (n 95) 4.

134 Earliest theorisations of cyberwar date back to the 1990s. Arquilla and Ronfeldt hypothesised and warned about the occurrence of cyberwar as early as 1993. In a widely reviewed RAND publication, they contended that 'the information revolution will cause shifts both in how societies may come into conflict, and how their armed forces may wage war', and proposed two related concepts to make sense of these developments: (a) netwar, which they considered to be 'societal-level ideational conflicts waged in part through internetted modes of communication', and (b) cyberwar, which they regarded as military-level hostilities, John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!' (1993) 12(2) Comparative Strategy 141 ⟨https://perma.cc/4JEZ-W5U8⟩, 144.

the mechanisms of cyberwar and cyberspace as a new realm of conflict, was Clarke's and Knake's publication *Cyber War: The Next Threat to National Security and What To Do About It*. Relying on personal reminiscences, Clarke, a former White House adviser, and Knake, a senior fellow for cyberpolicy at the Council on Foreign Relations, argued that there is a credible possibility that cyberwar may 'change the world military balance and thereby fundamentally alter political and economic relations'.[135] They further held that in order to mitigate the risks stemming from war-level cyberattacks, from a US perspective, it is critical to pursue, what they termed, a *defensive triad*, which refers to the (a) protection of the backbone of the internet, (b) the securing of critical infrastructures such as power grids, as well as the (c) fortification of defence networks.[136]

Rebutting Clarke's and Knake's assessments concerning the occurrence of cyberwar, Rid, in his seminal piece titled *Cyberwar Will Not Take Place*, argued that 'cyberwar is still more hype than hazard'.[137] Drawing on Clausewitzian criteria of war, i.e. that acts of aggression have to be potentially violent, purposeful, and political to classify as conflictual interactions, Rid maintained that the effects of nefarious cyberattacks had never amounted to acts of war in the past, that cyberwar does not occur in the present, and that the chances for cyberwar to take place in the future are slim.[138] Instead, he reasoned, the entirety of politically-motivated cyberassaults can best be understood as 'sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion'.[139]

---

135 R A Clarke and R Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins 2010) 53.

136 ibid. See also Valeriano and Maness, who developed a theory of cyberconflict, and analysed empirical patterns of contestation between different antagonists, Brandon Valeriano and Ryan C Maness, 'Cyber Conflict and Non-State Actors' in *Cyber War Versus Cyber Realities* (Oxford University Press 2015) ⟨https://perma.cc/K573-E6AQ⟩.

137 Thomas Rid and John Arquilla, 'Think Again: Cyberwar' [2012] (192) Foreign Policy 80 ⟨https://perma.cc/9CBL-NUTJ⟩, 80.

138 Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35(1) Journal of Strategic Studies 5 ⟨https://perma.cc/Q54H-PP5G⟩.

139 Ibid 5.

Rid's manifesto prompted a series of scholarly refutations, including by Arquilla and Stone, both of whom claimed that cyberwar had arrived, or is possible in the sense that cyberattacks can constitute acts of war as they can produce violent effects comparable to traditional forms of conflict.[140] With the intention of bringing debates about war in the virtual realm 'back down to earth', Gartzke provided a nuanced appraisal of the arguments advanced by cyberwar-critics and cyberwar-positivists.[141] Pursuing a middle ground, he posited that cyberwar can neither achieve conquest nor coercion as compellingly as existing modes of terrestrial force, and is hence best understood as an appendage to conventional warfare, 'or as a stop-gap and largely symbolic effort to express dissatisfaction with a foreign opponent'.[142] He also advanced that conflicts carried out in the digital domain are much more likely to increase existing military inequalities than to threaten dominant hierarchies.[143]

Debates about cyberwar also inspired discussions about cyberweapons and offensive capabilities, as well as scholarly exchanges about offence/defence balances and the prospects for effective deterrence and attribution in the virtual realm.[144] It has been

---

140 Rid and Arquilla (n 137); John Stone, 'Cyber War Will Take Place!' (2013) 36(1) Journal of Strategic Studies 101 ⟨https://perma.cc/43E6-XLAV⟩.

141 Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth' (2013) 38(2) International Security 41 ⟨https://perma.cc/VS92-3QMS⟩.

142 Ibid 73.

143 ibid. See also Green, who has engaged in a multidisciplinary analysis of cyberwarfare, James A Green, 'Introduction' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) ⟨https://perma.cc/7VWJ-3PZW⟩.

144 Tim Stevens, Cyberweapons: Governing the Ungovernable? (2016) ⟨https://perma.cc/4R7C-9REX⟩ accessed 30 November 2019; Tim Stevens, 'Cyberweapons: Power and the Governance of the Invisible' (2017) 55(3-4) International Politics 482 ⟨https://perma.cc/7S5A-BXXX⟩; Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons' (2018) 41(1-2) Journal of Strategic Studies 6 ⟨https://perma.cc/6WV2-V7G5⟩; Thomas Rid and Peter McBurney, 'Cyber-Weapons' (2012) 157(1) The RUSI Journal 6 ⟨https://perma.cc/JT6T-PHUD⟩; Jon R Lindsay, 'Stuxnet and the Limits of Cyber Warfare' (2013) 22(3) Security Studies 365 ⟨https://perma.cc/2X63-UJ9K⟩; Trey Herr, 'PrEP: A Framework for Malware and Cyber Weapons' (2013) 13(1) SSRN Electronic Journal ⟨https://perma.cc/BUM4-7AKB⟩; Trey Herr and Paul Rosenzweig, 'Cyber Weapons and Export Control: Incorporating Dual Use With the Prep Model' (2016) 8(2) Journal of National Security Law and Policy 301 ⟨https://perma.cc/NB6K-4EGL⟩; Trey Herr, 'Malware Counter-Proliferation and the Wassenaar Arrangement' (IEEE

widely contended that cyberspace complicates conventional logics of deterrence and attribution by virtue of its distributed, asymmetrical, anonymous, and dual use characteristics.[145] Specifically, it has been argued that networked ICTs provide militarily weaker agents with asymmetric advantages due to the fact that the barriers to obtain or build offensive capabilities are significantly lower compared to other weapons classes, and that, as a result of that, offensive actions are easier to uphold than defensive arrangements, and that various guises of technical anonymity undercut deterring efforts. Furthermore, it has been maintained that due to the fact that nefarious cyberactivities rely on the same open channels employed for communication purposes and commercial dealings, preventive or prescriptive measures fail to achieve necessary distinction.[146]

Scholars, including Gartzke and Lindsay, Fischerkeller and Harknett, as well as Tor have either disputed these conventional cyberrevolution arguments, or lobbied for less traditional approaches to deterrence and defence. In their 2017 publication, Gartzke and Lindsay, for example, called for a shift from deterrence to deception. They explained how deceptive strategies can improve protection, and call 'into question categorical assumptions about offence dominance'.[147] Similarly, Fischerkeller and

2016) ⟨https://perma.cc/32GS-JKRR⟩; Joseph SJr Nye, 'Nuclear Lessons for Cyber Security?' (2011) 5(4) Strategic Studies Quarterly 18 ⟨https://perma.cc/BUA8-GSMA⟩; Martin C Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation 2009); Jon R Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack' (2015) 1(1) Journal of Cybersecurity 53 ⟨https://perma.cc/QZ7B-WQEU⟩; Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (Aegis Paper Series No. 1607, 2016); Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38(1-2) Journal of Strategic Studies 4 ⟨https://perma.cc/EV3G-NSEH⟩; Erik Gartzke and Jon R Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace' (2015) 24(2) Security Studies 316 ⟨https://perma.cc/22M3-W3PJ⟩; Nigel Inkster, 'Measuring Military Cyber Power' (2017) 59(4) Survival 27 ⟨https://perma.cc/FM48-TGYT⟩.

145 Chelsey Slack, 'Wired yet Disconnected: The Governance of International Cyber Relations' (2016) 7(1) Global Policy 69 ⟨https://perma.cc/KR29-XE9X⟩.

146 Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press 2011); Mike McConnell, 'Cyberwar Is the New Atomic Age' (2009) 26(3) New Perspectives Quarterly 72 ⟨https://perma.cc/XSQ6-RS36⟩; Clarke and Knake (n 135); Nye, 'Nuclear Lessons for Cyber Security?' (n 144); Masashi Crete-Nishihata and Ronald J Deibert, 'Global Governance and the Spread of Cyberspace Controls' (2012) 339(18) Global Governance 339 ⟨https://perma.cc/MEL2-7X6G⟩; Kramer (n 87).

147 Gartzke and Lindsay (n 144) 319.

Harknett, as well as Tor, advocated for alternative approaches to deterrence, namely for strategies of cyberpersistence and cumulative deterrence, respectively. The former argued that '[i]n an environment of constant contact, a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behaviour'.[148] Tor, in turn, put forward that in order to shape and limit acts of cyberaggression, it is necessary to attack perpetrators 'repeatedly in response to specific behaviours, over a long period of time, sometimes even disproportionally to [their] aggressive actions'.[149]

Mounting concerns about nefarious cyberactivities, also inspired great numbers of legal commentaries and assessments seeking to influence and shape doctrines and frameworks.[150] Questions, including but not limited to whether there are permissible uses of offensive cybercapabilities, whether extant international legal provisions can adequately structure and govern these capabilities, and whether states can lawfully exert legal authority in response to cyberattacks carried out by public and private offenders have been at the forefront of international legal endeavours.[151] In his 2011 publication

---

148 Michael P Fischerkeller and Richard J Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace' (2017) 61(3) Orbis 381 ⟨https://perma.cc/B3CL-2TNZ⟩, 381.

149 Uri Tor, ''Cumulative Deterrence' as a New Paradigm for Cyber Deterrence' (2017) 40(1-2) Journal of Strategic Studies 92 ⟨https://perma.cc/Q8EF-T5GH⟩, 95.

150 These assessments can be seen 'as part of a long-standing tradition of legal scholars and practitioners labouring to adapt existing law to new circumstances, opting to extend the law by way of interpretation and analogy rather than by developing a brand new legal paradigm', Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) American Journal of International Law 583 ⟨https://perma.cc/FSU5-FUJ6⟩, 583.

151 Kristen E Eichensehr, 'Review of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)' (2014) 108 American Journal of International Law 585 ⟨https://perma.cc/M8ZG-QS6H⟩; Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' [2012] (September 2011) 4th International Conference on Cyber Conflict 91 ⟨https://perma.cc/PNN2-JXL4⟩; Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36(2) Yale Journal of International Law 421 ⟨https://perma.cc/BF5K-D83Y⟩; Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (techspace rep, NATO Cooperative Cyber Defence Centre of Excellence 2010) ⟨https://perma.cc/7XMT-5YCA⟩; Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal Online 2 ⟨https://perma.cc/B7TJ-55U5⟩; Catherine Lotrionte, 'Reconsidering the

Waxman, for instance, contended that while violent cyberassaults 'pose difficult line-drawing problems' in the sense that they raise intricate questions about 'permissible versus impermissible modes of interstate conduct and conflict', it is not impossible to conceptualise strategic legal solutions around these issues.[152] He suggested that

> some problems of cyberwarfare for regulating force are at the same time unique yet familiar. Viewing these questions in the context of Cold War debates about the [United Nations] Charter and its prohibition of force highlights that although the technology of conflict, both in terms of capabilities and probable vulnerabilities, is changing in revolutionary ways, many of the interrelated strategic and legal challenges that arise are not new.[153]

Hathaway and others provided comprehensive evaluations of how existing legal provisions issued by national as well as international bodies 'may be applied, and adapted and amended, to meet the distinctive challenge[s] posed by cyberattacks'.[154] Following thorough reviews of jus ad bellum (i.e. when does nefarious conduct in cyberspace reach the threshold of an armed attack justifying measures of retaliatory self-defence in line with Article 51 of the United Nations Charter) and jus in bello questions (i.e. how do the laws governing behaviour in the course of violent hostilities apply to offensive cyberactivities), Hathaway and others came to the conclusion that existing legal frameworks only effectively address 'a small fraction of potential cyberattacks'.[155] They argued that jus ad bellum and jus in bello provisions respectively, provide guidelines 'for responding only to those cyberattacks that amount to an armed attack or that take place in the context of an ongoing armed conflict'.[156] In line with

---

Consequences for State-Sponsored Hostile Cyber Operations Under International Law' (2018) 3(2) The Cyber Defense Review 73 ⟨https://perma.cc/8VTM-CMCJ⟩.

152 Waxman (n 151) 458.

153 Ibid 458.

154 Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100(4) California Law Review 817 ⟨https://perma.cc/642V-LXA3⟩, 817.

155 Ibid 817.

156 Ibid 817.

their findings, the investigators called for the enactment of new, more inclusive legal instruments at both domestic and international levels.[157]

Two of the most comprehensive assessments concerning the application of lex lata provisions to cyberattacks were conducted by two groups of distinguished legal academics, under the directorship of *Exeter Law School Professor* and *Chairman of the Stockton Center for the Study of International Law at the United States Naval War College*, Michael N. Schmitt, between 2009-2013 and 2013-2017, respectively. Invited by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), the two International Groups of Experts (IGEs) issued two Manuals, the *Tallinn Manual on the Law of Cyberwarfare* and the *Tallinn Manual 2.0 on the International Law of Cyberoperations*, which elucidate how existing international legal provisions relate to the realities of the virtual realm.[158] In contrast to the first edition, which was exclusively concerned with how international legal frameworks, in particular jus ad bellum and jus in bello rules and principles, apply to hostile cyberactivities and govern the use of cyberforce by states, the second edition of the Tallinn Manual pursued a broader mandate and also looked at international legal doctrines regulating cyberactivities occurring in peacetime (i.e. malicious cyberactivities below the threshold of armed conflict, which arguably constitute the vast majority of nefarious cyberactivities).[159]

---

[157] Hathaway and others noted that applying the laws regulating the conditions for going to war as well as the behaviour of warring entities to the digital domain is exceptionally challenging. 'The key treaties governing conduct in war, the Geneva Conventions, were last revised in the wake of World War II. Nothing was further from the minds of the drafters of the Geneva Conventions than attacks carried out over ... worldwide computer network[s]. [For example,] [o]ne unanticipated challenge is how to address attacks that have little or no direct physical consequences, but that nonetheless cause real harm to national security', see Hathaway and others (n 154) 840.

[158] Michael N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Michael N Schmitt ed, Cambridge University Press 2013) ⟨https://perma.cc/A829-LAC8⟩; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N Schmitt ed, Cambridge University Press 2017) ⟨https://perma.cc/C42C-QVVE⟩; Michael N Schmitt, Factsheet: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017) ⟨https://perma.cc/7WD2-NNX6⟩ accessed 27 March 2018.

[159] Efrony and Shany (n 150). The first edition of the Tallinn Manual produced 95 black letter rules

Neither the first nor the second version of the Tallinn Manual were envisaged to create binding international law. Rather, as noted in the introduction to the Tallinn Manual 2.0, the outputs produced were intended to reflect 'the opinions of the two International Groups of Experts as to the state of the law'.[160] The Manuals are neither best-practice guides nor progressive legal reform attempts but strive to be policy and politics-neutral. They are objective restatements of lex lata provisions.[161] Both editions of the Tallinn Manual generated considerable reactions by scholars and policymakers alike, and will be further analysed apropos their detailed content and effectiveness in *Chapter 4*.

Against the background of mounting concerns about violent confrontations in cyberspace, and building on the insights gathered by Waxman, Hathaway, as well as the legal experts contributing to the Tallinn Manuals, Eichensehr, in her 2015 publication, sought to answer three pertinent questions: (a) what role, if any, should private actors play in the governance of the virtual realm, (b) how should cyberspace be governed, i.e. which instruments should be employed (no governance framework, treaty provisions, or norms), and (c) how should military activities be regulated.[162] Drawing analogical parallels to the histories of the high seas, outer space, and Antarctica, she reasoned that 'states can develop governance mechanisms for domains that, by necessity or agreement, are not partitioned and governed by traditional territorial sovereignty'.[163] With regard to controlling nefarious activities in cyberspace, she maintained that,

---

pertaining to cyberwarfare, which were intended to restate existing doctrines. The second edition of the Tallinn Manual introduced 154 rules and presented 'the general legal principles governing cyberoperations and their interaction with specialised international law regimes, such as human rights law, diplomatic law, space law, and telecommunication law', Efrony and Shany (n 150) 584.

160 Factsheet: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (n 158) 2.

161 Ibid.

162 Eichensehr, 'The Cyber-Law of Nations' (n 15).

163 Ibid 380.

in contrast to other domains, 'the historical and ongoing role of private parties in the governance, use, and ownership of the [i]nternet and its underlying architecture suggests that [a] multistakeholder model is preferable to a purely multilateral model'.[164] She further suggested that given the absence of stringent customary provisions as well as the starkly diverging conceptions/visions of cyberspace among Eastern and Western proponents and their relevant allies, the enactment of treaty instruments for the virtual realm appears highly unlikely, and that governance should instead be pursued via norms. In addition, Eichensehr purported that sovereign entities should address tendencies of militarisation by means of 'translating existing laws of armed conflict to cyber[space] and considering additional cyberspecific rules'.[165]

2.2 Norms

In the context of promoting responsible behaviour in cyberspace, norms 'have emerged along with confidence- and capacity-building measures as the principal policy tools of choice to meet the ... vision of an open, secure, accessible, and peaceful ICT environment'.[166] Similar to the concepts introduced earlier in this chapter (i.e. cyberspace and cybersecurity), norms appear to effectuate comparable definitional quarrels. As theoretical constructs, norms have been addressed across a broad range of scholarly literatures, including across sociology, philosophy, economics, communication and environmental studies, as well as political science and law literatures. Accordingly, a multitude of characterisations and approaches concerning norms have developed.[167] Among other things, norms have been put on par with or understood as social facts,

164 Eichensehr, 'The Cyber-Law of Nations' (n 15) 380.

165 Ibid 380.

166 Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (n 20) 10.

167 Sophie Legros and Beniamino Cislaghi, 'Mapping the Social-Norms Literature: An Overview of Reviews' (2020) 15(1) Perspectives on Psychological Science 62 ⟨https://perma.cc/UG57-JEHT⟩.

principles or legal rules.[168] Although these concepts share some theoretical intersections with norms as conceived by this thesis, they exhibit different structural determinants (please refer to the remarks in the next section *Governing Through Shared Expectation* for more details). Being aware of the array of different theoretical perceptions surrounding norms is useful with regards to (potentially) making out stakeholder-related differences in understandings concerning their enforceability, as well as variations in corresponding pictures of law/society relations (or the legal organisation of society). For instance, differences in conceptions of norms may go hand in hand with differences in degrees of legal pluralism. That is to say, broader understandings of norms as standards of appropriate behaviour propagated by a multiplicity of actors may inspire stronger legal pluralism, whereas narrower perceptions of norms, which rely on validation by state organs, may result in weaker legal pluralism.[169]

Conscious of these definitional challenges, this thesis considers norms to constitute 'collective expectations for the proper behaviour of actors with a given identity', or 'shared understandings that make behavioural claims'.[170] Cybersecurity norms, by extension, can be defined as collective expectations of appropriate behaviour vis-à-vis maintaining global security and stability of cyberspace.[171]

---

168 Erskine and Carr (n 37); Steven Wheatley, 'Democratic governance beyond the state: the legitimacy of non-state actors as standard setters' in Anne Peters and others (eds), *Non-State Actors as Standard Setters* (Cambridge University Press 2009) ⟨https://www.cambridge.org/core/product/identifier/CBO9780511635519A023/type/book_part⟩; Wayne Sandholtz, *International Norm Change* (Oxford University Press 2017) ⟨https://perma.cc/8629-CB4Z⟩.

169 John Griffiths, 'What is Legal Pluralism?' (1986) 18(24) Journal of Legal Pluralism and Unofficial Law 1 ⟨https://perma.cc/C5V5-KJN5⟩; Brian Z Tamanaha, 'The Folly of the 'Social Scientific' Concept of Legal Pluralism' (1993) 20(2) Journal of Law and Society 192 ⟨https://perma.cc/9YL7-DAAL⟩.

170 Peter J Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press 1996); Jeffrey T Checkel, 'Norms, Institutions, and National Identity in Contemporary Europe' (1999) 43(1) International Studies Quarterly 83 ⟨https://perma.cc/ZA9H-BA76⟩; Finnemore and Sikkink (n 43) 5.

171 Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' [2019] Hague Journal on the Rule of Law ⟨https://perma.cc/47E3-8VH7⟩; Martha Finnemore, 'Cultivating International Cyber Norms' in Kristin M Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age* (Center for a New American Security 2011) ⟨https://perma.cc/CBZ2-PHT4⟩.

Norms define legitimate social purposes that enable or constrain the behaviour of actors. As expectations rather than binding commitments, norms encourage broad membership and participation.[172] Actors hesitant to adhere to formal legal obligations may display greater inclination to subscribe to voluntary (sets of) norms.

> Over time, these initially reluctant states, firms and individuals may become socialised into deeper acceptance of the norms. Compliance becomes internalised as [they] get used to the expectations, see their utility and come to share them more fully than they did [at the outset].[173]

Both international relations and international law research have developed close familiarity with norms, empirically as well as theoretically.[174] Since the end of the Cold War, constructivist international relations scholarship, in particular, has made important contributions to advancing analytically more rigorous understandings of shared expectations of appropriate conduct at domestic and global levels.[175] Early scholarly works mainly focused on providing analytical counterweights to predominantly structural and rational conceptions of international politics.[176] Academic contributions produced during this phase sought to demonstrate the implications of norms on domestic and international outcomes.[177] Subsequent research zoomed in on processes of norm emergence and diffusion, and developed relevant theories, including transnational

---

172 Finnemore, 'Cultivating International Cyber Norms' (n 171).

173 Ibid 90.

174 Jutta Brunnée and Stephen J Toope, 'Constructivism and International Law' in Jeffrey L Dunoff and Mark A Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations* (Cambridge University Press 2013) ⟨https://perma.cc/ZN62-NCZA⟩.

175 Checkel, 'Norms, Institutions, and National Identity in Contemporary Europe' (n 170).

176 Hoffmann (n 43).

177 Alexander Wendt, 'The Agent-Structure Problem in International Relations Theory' (1987) 41(3) International Organization 335 ⟨https://perma.cc/H88V-XHMZ⟩; Nicholas G Onuf, *World of Our Making: Rules and Rule in Social Theory and International Relations* (University of South Carolina Press 1989); Friedrich Kratochwil and John Gerard Ruggie, 'International Organization Foundation International Organization: A State of the Art on an Art of the State' (1986) 40(4) International Organization 753 ⟨https://perma.cc/M5ZX-N7UJ⟩; Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations' (n 77).

actor models and legalisation approaches.[178] Among those theories, Finnemore's and Sikkink's *norm life cycle* and Risse-Kappen's, Ropp's, and Sikkink's *spiral model*, respectively acquired particular prominence.[179]

Seeking to explain the emergence of and change in shared beliefs, the frameworks advanced by Finnemore and Sikkink, and Risse-Kappen, Ropp, and Sikkink, respectively considered normative socialisation processes to be the results of pressure politics at the global level. Finnemore and Sikkink, and Risse-Kappen, Ropp, and Sikkink, respectively put forward that norms are moulded by so-called *norm activists* or *entrepreneurs* that mobilise civil society groups or networks within and across states to back their normative ideas. As normative pressure and persuasion are exerted from above (transnationally) and below (domestically), and more parties, including sovereign entities, start to subscribe to the principled ideas advocated (subsequent to initial periods of repression

---

178 Sandholtz (n 168); Finnemore and Sikkink (n 43); Thomas Risse-Kappen, Stephen C Ropp, and Kathryn Sikkink, *The Power of Human Rights: International Norms and Domestic Change* (Cambridge Studies in International Relations, Cambridge University Press 1999); Anne-Marie Slaughter, Andrew S Tulumello, and Stepan Wood, 'International Law and International Relations Theory: A New Generation of Interdisciplinary Scholarship' (1998) 92(3) The American Journal of International Law 367 ⟨https://perma.cc/F5Y6-92Z7⟩; Stephen J Toope, 'Emerging Patterns of Governance and International Law' in Michael Byers (ed), *The Role of Law in International Politics* (Oxford University Press 2001) ⟨https://perma.cc/W6PZ-844D⟩.

179 Finnemore and Sikkink (n 43); Risse-Kappen, Ropp, and Sikkink (n 178). The norm life cycle as devised by Finnemore and Sikkink sees norms develop along three key stages, (a) emergence, (b) cascade (broad acceptance), and (c) internalisation, Finnemore and Sikkink (n 43) 896. Stages one and two are divided by a tipping point, a juncture, at which a critical mass of actors subscribe to the principled ideas advocated. 'Internalised or cascading norms may eventually become the prevailing standard[s] of appropriateness against which new norms emerge and compete for support', ibid 895. The completion of all three stages is not inevitable. It may well be that principled beliefs fail at either one of the three stages and do not emerge, cascade, or become taken for granted. The spiral model denotes an ideal-typical five-stage model formulated to explain normative socialisation processes. The five stages as defined by Risse-Kappen, Ropp, and Sikkink include (a) repression, (b) denial, (c) tactical concessions, (d) prescriptive status, and (e) rule-consistent behaviour. The model specifies the prevailing logics of action and casual mechanisms present in each one of the five phases and emphasises interactions between normative forces at domestic and international levels. Progress towards implementation is achieved with every phase completed. 'The spiral model ascribes great magnitude to psycho-social factors in [processes] of change. Processes of shaming and denunciation lead first to strategic concessions. However, later on the changes acquire ... binding status, as governments and people go through processes of internalisation and habituation [towards] universal norms', Eran Shor, 'Conflict, Terrorism, and the Socialization of Human Rights Norms: The Spiral Model Revisited' (2008) 55(1) Social Problems 117 ⟨https://perma.cc/CTW3-J73T⟩, 121.

and denial), they cross a tipping point and begin to cascade/spiral, and eventually become internalised and taken for granted.[180] In the remit of these theories, non-state actors were deemed to be critical players for helping norms emerge through advocacy, and inciting formal legal debates (particularly during the early stages of norm development processes).[181]

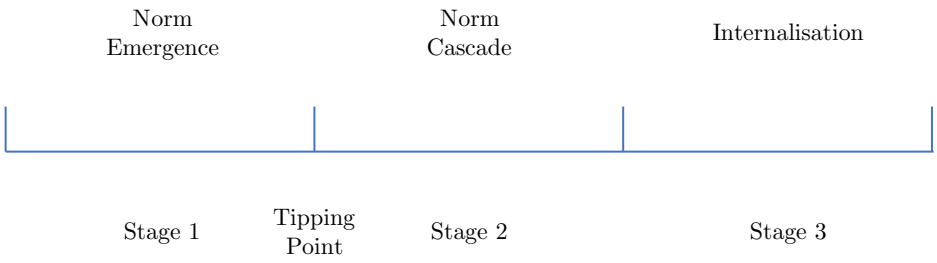

Figure 2.1: The Norm Life Cycle, see Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998) 52(4) International Organization 887 ⟨https://perma.cc/7CWG-H7JE⟩.

Later scholarly works criticised these models for their relatively static and uni-directional/deterministic conceptions of norms and related processes of change, and instead focused on examining the inherently dynamic aspects of 'norms and norm systems'.[182] Scholars, including Wiener and Sandholtz, contended that norms do not remain uncontested, and that they evolve as much through transnational advocacy activities as they do through cycles of application and debate. As such, norms are both stable and flexible, and exhibit a dual nature.[183] Once established as social facts, norms shape conduct and demeanour. At the same time, however, their content and

---

180 Finnemore and Sikkink (n 43); Risse-Kappen, Ropp, and Sikkink (n 178); Sandholtz (n 168).

181 Finnemore and Sikkink (n 43).

182 Sandholtz (n 168) 6. 'Norms were conceptualised as having specific behavioural strictures (a relatively bounded set of appropriate behaviours) that did not change', Hoffmann (n 43) 5.

183 Antje Wiener, 'The Dual Quality of Norms and Governance Beyond the State: Sociological and Normative Approaches to Interaction' (2007) 10(1) Critical Review of International Social and Political Philosophy 47 ⟨https://perma.cc/DUD5-WRCR⟩; Antje Wiener, *The Invisible Constitution of Politics: Contested Norms and International Encounters* (Cambridge University Press 2008).

validity may be challenged at any point in time, leading to contestation and different types of behaviour (including regression).[184]

2.2.1 Governing Through Shared Expectations

Functionally, norms serve different purposes. Kratochwil, for instance, argued that 'norms are used to make demands, rally support, justify action, ascribe responsibility, and assess the praiseworthy or blameworthy character of an action'.[185] Cortell and Davis considered norms to provide solutions to global coordination problems, reduce transaction costs, and offer 'a language and grammar of international politics'.[186] Ferguson maintained that 'by shaping agents' understandings of their social environments, associated interactions, and possible outcomes', norms choreograph/align activities, foster predictability, and help reduce contextual ambiguity and uncertainty to manageable levels.[187] Norms exhibit both regulative and constitutive characteristics. With their emergence in socially predicated contexts, norms promote and assign values, shape expectations and interests, and create meanings, which in turn affect the social identities of actors and actions (constitutive).[188] At the same time, they define legitimate courses of action and behavioural prescriptions, and impose constraints (regulative).

---

184 Antje Wiener, *A Theory of Contestation* (Springer 2014); Lisbeth Zimmermann, Nicole Deitelhoff, and Max Lesch, 'Unlocking the Agency of the Governed: Contestation and Norm Dynamics' (2017) 2(5) Third World Thematics: A TWQ Journal 691 ⟨https://perma.cc/379P-5DYA⟩; Xymena Kurowska, *The Politics of Cyber Norms: Beyond Norm Construction* (techspace rep, EU Cyber Direct 2019) ⟨https://perma.cc/B67N-JM2T⟩.

185 Friedrich Kratochwil, 'The Force of Prescriptions' (1984) 38(4) International Organization 685 ⟨https://perma.cc/KPH5-G5WZ⟩, 686.

186 Andrew P Cortell and James W Davis Jr, 'Understanding the Domestic Impact of International Norms: A Research Agenda' (2000) 2(1) International Studies Review 65 ⟨https://perma.cc/ERU5-9DLG⟩, 66.

187 William D Ferguson, 'Facing Uncertainty: The Role of Norms and Formal Institutions as Shared Mental Models' (SASE Mini-Conference on Uncertain Futures in Economic Decision Making, London, 2019) ⟨https://perma.cc/YFD2-39G3⟩ 1.

188 Wiener, *The Invisible Constitution of Politics: Contested Norms and International Encounters* (n 183); Wiener, *A Theory of Contestation* (n 184); Alexander Wendt, *Social Theory of International Politics* (Cambridge University Press 1999).

Conceptually, norms unite three key elements. As per Winston, they serve as nexus between (a) problem sets, (b) values, and (c) behaviours.[189] Norms respond to issues which demand attention. The remediating actions/behaviours taken with regard to addressing the problem sets under consideration are, in turn, informed by different value postures held by different actors. Conceptually, norms can thus be formalised as follows: If [problem sets], [values] suggest [behaviours].[190] To illustrate, in instances of nefarious cyberattacks crossing the threshold of use of force (problem set), widely shared understandings expressed in International Humanitarian Law, e.g. principles of distinction and proportionality (values), would suggest non-use of indiscriminate offensive cybercapabilities (behaviour).

Structurally, norms differ from, yet share links to concepts such as laws or principles. Principles tend to be phrased in highly general terms and rarely set out clear actor responsibilities apropos achieving behavioural goals. As such, they are not 'outcome determinative'.[191]

> Pursuing agreement on principles, as opposed to norms, may be politically attractive precisely because it allows some fudging about behavioural obligations. Articulating specific obligations for specific actors (that is, articulating norms) invites scrutiny and claims of accountability in ways that principles do not. For that reason, constructing norms may be more controversial. Of course, this is also why norms can be more valuable as policy tools.[192]

In contrast to laws, norms typically display broader framings. In line with higher levels of specificity, laws also characteristically carry greater coercive power. 'At the same time, laws are not entirely autonomous from norms; most forms of law are

---

189 Carla Winston, 'Norm Structure, Diffusion, and Evolution: A Conceptual Approach' (2018) 24(3) European Journal of International Relations 638 ⟨http://perma.cc/76X3-A348⟩.

190 Ibid 641.

191 Finnemore and Hollis (n 45) 441.

192 Martha Finnemore, 'Cybersecurity and the Concept of Norms' (Carnegie Endowment for International Peace, 2017) ⟨https://perma.cc/K7QA-UL6G⟩ 2.

bolstered by a strong element of normativity. Indeed, many laws aim to create norms by using the legitimacy of law to define shared expectations'.[193]

In addition to strategic political considerations, the move to voluntary norms of responsible behaviour to increase the stability of the virtual realm can partly be attributed to concerns over the suitability and effectiveness of binding treaties for cyberspace, as well as to fears of legal lock-in among leading cyberpowers, and difficulties of attribution.[194] In circumstances characterised by high levels of uncertainty, that is, in situations 'when even the range and/or distribution of possible outcomes is unknown', the conclusion of formal legal agreements may not seem attractive.[195] 'In particular, if actors are ambiguity-averse, they will prefer to leave agreements imprecise rather than face the possibility of being caught in unfavourable commitments'.[196]

2.2.2 Constructing Rules of the Road for the Virtual Realm

Although scholarly works studying norms of responsible behaviour in cyberspace have increased in numbers and analytical depth over the past years, the scope of publications pertaining to rules of the road for the virtual realm has remained fairly narrow.[197]

---

193 Finnemore, 'Cybersecurity and the Concept of Norms' (n 192) 2. Sandholtz, for instance, proposed that '[r]ules and norms are not different things. Both are standards of conduct for a set of actors in a given context. Norms (and rules) vary in formality, specificity, and organised enforcement. Clarity will be served by recognising that norms and rules are the same thing (standards of conduct) and then identifying the levels of specificity and formality of particular norms when it is important to do so. For example, laws are a subcategory of norms with a high level of formality, created through processes recognised as *legal*. Laws also vary widely in specificity and organised enforcement', see Sandholtz (n 168) 3.

194 Henry Farrell, *Promoting Norms for Cyberspace* (techspace rep, April, 2015) ⟨https://perma.cc/T9ER-5935⟩; Finnemore, 'Cybersecurity and the Concept of Norms' (n 192); Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (n 171).

195 Kenneth W Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54(3) International Organization 421 ⟨https://perma.cc/584R-7QB7⟩, 442.

196 Ibid 442.

197 For a useful overview of cybersecurity norms-related outputs, please refer to the list of publications maintained by the *The Hague Program for Cyber Norms*, see https://perma.cc/D8TD-5W9N.

Inspired by recommendation (i) of the 2010 UN GGE report, i.e. to '[f]urther dialogue among states to discuss norms pertaining to state use of ICTs, to reduce collective risk and protect critical national and international infrastructure', a group of academics, policymakers, and cybersecurity practitioners at Harvard University, Massachusetts Institute of Technology, and the University of Toronto launched a workshop series intended to elaborate possible contents of such norms.[198] The subject matter experts concluded their work with five candidate norms, which they believed would attract widespread support. The candidate norms issued, called on states to (a) distinguish between disruptive and damaging cyberattacks, and to (b) assist other states in cases of attacks and disasters. The norms further asked governments to (c) create certification schemes for digital supply chains, (d) share intelligence pertaining to cybercriminal activities (law-enforcement cooperation), and (e) pursue public-private partnerships locally and globally. According to the workshop participants, the norms devised were status quo-oriented and were geared towards 'reducing vulnerability and confrontation rather than ... suppressing threat actors'.[199]

Similarly intrigued by the outcomes of the 2010 iteration of the UN GGE, Maurer examined norm emergence processes in the remit of the United Nations and traced corresponding dynamics. He identified two principal streams of negotiation concerned with bringing into existence standards of expected behaviour in cyberspace, (a) a politico-military stream focusing on cyberwarfare and (b) an economic stream focusing on cybercrime.[200] Employing Finnemore's and Sikkink's norm life cycle concept, he argued that 'norms to govern cyberspace are slowly emerging and moving towards

---

198 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 23) 18.

199 Roger Hurwitz, *An Augmented Summary of the Harvard , MIT and University of Toronto Cyber Norms Workshop* (techspace rep, Massachusetts Institute of Technology 2012) ⟨https://perma.cc/QX9P-NFFZ⟩ 23.

200 Tim Maurer, *Cyber Norm Emergence at the United Nations* (techspace rep, September, The Belfer Center for Science and International Affairs 2011) ⟨https://perma.cc/6SNR-5DX9⟩ 6.

norm cascade'.[201] Even a decade later, Maurer's assessment still holds true. Since the publication of his report and as a result of high levels of normative contestation among political elites, norms have only marginally moved closer to cascading.

Taking note of increasing levels of technological pervasiveness and lurking questions of global coordination, Finnemore analysed 'the tasks involved in cultivating new norms and rules for cyberspace'.[202] Resorting to insights from other policy areas (e.g. trade and climate change), she identified different factors which help norm-making efforts bear fruit. 'Successful norms are likely to be simple and clear, obviously useful and relatively easy to follow', she maintained.[203] She further held that there is merit in *grafting* cybersecurity-related behavioural expectations to existing legal regimes and normative frameworks, creating multi-pronged promotion strategies, and linking norms and laws in a complimentary fashion.[204] Although simple and easy to follow normative stipulations may be conducive to increased compliance, it is worth noting that overly simple rules may be subject to gaming and de facto circumvention, which has led scholars, including McBarnet and Whelan, to support broad-based standards.[205] The latter, it has been argued, 'are more likely to produce behaviour which fulfils the regulatory objectives' and inhibit creative compliance.[206]

Employing insights from regime theory, Nye conducted a mapping exercise of key cybersecurity governance activities and unveiled fragmented processes or what scholars have come to label a *regime complex*. Rather than on the bases of coherent, integrated

---

201 Maurer, *Cyber Norm Emergence at the United Nations* (n 200) 6.

202 Finnemore, 'Cultivating International Cyber Norms' (n 171) 89.

203 Ibid 89.

204 Ibid.

205 Doreen McBarnet and Christopher Whelan, 'The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control' (1991) 54(6) The Modern Law Review 848 ⟨https://perma.cc/X49D-94KH⟩.

206 Julia Black, Martyn Hopper, and Christa Band, 'Making a Success of Principles-Based Regulation' (2007) 1(3) Law and Financial Markets Review 191 ⟨https://perma.cc/NRR2-MZCU⟩, 193.

steering mechanisms, global activities pertaining to cybersecurity are governed by 'loosely coupled norms and institutions that [rank] somewhere between ... hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages', he argued.[207] Nye submitted that the emergence of tightly integrated coordination mechanisms for cybersecurity-related policy areas is questionable. Rather, he held, instances of fragmentation are likely to persist and disperse further.[208]

Echoing notions of complexity, Erskine and Carr, in their publication titled *Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace*, explored the difficulties and prospects of understanding existing and cultivating new norms in cyberspace.[209] They posited that for norm creation projects

> to be effective it is not only proposed principles or codes of conduct that must be the objects of such efforts. Rather, the broader systems of underlying values in which norms necessarily emerge and are embedded must also be the focus of analysis, and possibly persuasion, negotiation and concerted attempts at revision over time. Neglect of the complex contexts in which international norms must be situated leads to the promotion of quasi-norms, which may be clear statements of preferred principles on the part[s] of certain actors, but lack the prescriptive force and collective acceptance that make norms so powerful in international relations.[210]

Kurowska in her 2019 publication *The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation* examined norm formation efforts through contestation-oriented lenses.[211] She maintained that traditional approaches to norm construction, focused on socialisation and compliance, have the potential to increase the likelihood of norm backlash and recoil. Instead, and to better respond to the political actualities surrounding cybersecurity norm development projects, actors

---

207 Nye, 'The Regime Complex for Managing Global Cyber Activities' (n 37) 7.

208 Ibid.

209 Erskine and Carr (n 37).

210 Ibid 108.

211 Kurowska (n 184).

should pursue conscious strategies of narrative contestation, she argued. Kurowska put forward that processes of contestation introduce elements of 'continuous difference, mutual learning and co-creation of norms', which can render norm creation efforts, in particular persuasion-oriented efforts, more 'meaningful' and robust.[212] In contexts premised on processes of strategic narrative contestation, 'all can tell their stories. But some stories are better than others and can also be better told'.[213]

Following the non-consensus outcome of the 2017 UN GGE discussions, Grigsby declared the end for norms of responsible behaviour in cyberspace. 'The development of norms had a good run', he asserted.[214] Against the background of political contentions surrounding discussions about rules of the road for the digital domain, particularly with regard to the applicability of International (Humanitarian) Law to cyberspace, he suggested abandoning norms-related discussions, and instead directing attention to confidence building measures (CBMs). Confidence building measures are transparency increasing actions undertaken by antagonists with a view to establishing trust relationships (in an incremental fashion). Typical examples of confidence building measures include the installation of crisis hotlines or the exchange of doctrines. In contrast to norms, CBMs do not demand shared ideological principles but rely on practical measures for progress in situations of disagreement and potential escalation.

Henriksen, too, proclaimed the 'end of the road for the UN GGE process', and reasoned that the non-report result of the 2017 UN GGE is likely to contribute to heightened levels of normative fragmentation and 'a shift away from ambitious global initiatives ... towards regional agreements between *like-minded states*'.[215] He also saw

---

212 Kurowska (n 184) 11.

213 Ibid.

214 Alex Grigsby, 'The End of Cyber Norms' (2017) 59(6) Survival 109 ⟨https://perma.cc/Z3EX-FPJS⟩, 119.

215 Henriksen (n 18) 2.

more prominent roles for non-state actors to bring (much needed) instances of clarity and advancement to cybersecurity governance processes.

Despite the death proclamations issued, norms-oriented discussions did not subside post-2017. On the contrary, the months ensuing the non-consensus outcome of the 2017 UN GGE saw the appearance of various norms proposals initiated by non-state actors.[216] Taking note of these developments, Hurel and Cruz Lobato engaged in a review of the norm promotion endeavours conducted by Microsoft. Reviewing primary policy outputs and strategies, they claimed that technology companies such as Microsoft seek to actively influence global courses of action pertaining to cybersecurity.[217]

Gorwa and Peez also scrutinised the cybersecurity-focused norm-building activities conducted by Microsoft, in particular the company's efforts surrounding the Cybersecurity Tech Accord. With a view to identifying the drivers behind Microsoft's normative undertakings, they stated that the latter need to be understood in the context of Microsoft's loss of consumer confidence resulting from its participation in the PRISM surveillance programme between 2007-2013.[218] According to Gorwa and Peez, Microsoft's undertakings primarily represent attempts at levelling the playing field among competitors and exhibit elements of 'rationalist calculations'.[219]

---

[216] For a concise summary of key private sector initiatives relating to cybersecurity norms, please refer to Hinck's blog post and Eggenschwiler's research paper, see Garrett Hinck, Private-Sector Initiatives for Cyber Norms: A Summary (2018) ⟨https://perma.cc/MR4K-VR4K⟩ accessed 25 June 2018; Jacqueline Eggenschwiler, *International Cybersecurity Norm Development: The Roles of States Post-2017* (techspace rep, April, EU Cyber Direct 2019) ⟨https://perma.cc/7PR4-C72T⟩.

[217] Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs' (2018) 3(1) Journal of Cyber Policy 61 ⟨https://perma.cc/F3QL-LKKG⟩.

[218] Robert Gorwa and Anton Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' [2018] SocArXiv ⟨https://perma.cc/G9TB-QPB2⟩.

[219] Gorwa and Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' (n 218); Annegret Flohr and others, *The Role of Business in Global Governance* (Palgrave Macmillan UK 2010) ⟨https://perma.cc/LN24-QTY3⟩.

For Mačák the increase in non-state actor-driven norms proposals pointed towards several problems at the heart of formal cybersecurity law-making processes. He maintained that the reluctance of states to consider binding international treaties, and their hesitation to voice their opinions on 'specific interpretations of controversial legal questions' has led to interpretation and power vacuums, which are being filled by non-state actors.[220] While trends of pluralisation related to law-making processes should not be read as unsettling per se, according to Mačák, he encouraged governments to reclaim their law-making positions. If states want to avoid existing vacuums being exploited to their disadvantage, that is to 'upset their ability to achieve strategic and political goals', they are well-advised to get back in the game and act in a timely fashion, Mačák argued.[221]

In line with Carr's and Erskine's, Finnemore's and Hollis', as well as Kurowska's remarks, this thesis submits that in terms of analysing norm formation processes, it is important to remember that process-related components are as important to normative stipulations as their substantive contents.

> Norms are not deracinated abstractions; they do not come about by fiat or desire, and they are never imposed in a vacuum. Norms are social creatures that grow out of specific contexts via social processes and interactions among particular groups of actors.[222]

Process-oriented analyses are critical for elucidating different actors involved in norm creation projects, their motivations, as well as the relevant social and organisational

---

220 Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (n 16).

221 ibid 23. Offering an outlook, Mačák held that '[i]t appears that at least some state representatives already realise that compliance with international law frees them to do more, and do more legitimately, in cyberspace. It remains to be seen whether this awareness will spread and gradually translate into states' general willingness to also shape the content of the law by reclaiming their traditional central legislative role in this area', see ibid 23.

222 Finnemore and Hollis (n 45) 427.

platforms involved in putting forward rules of the road for the virtual realm.[223] 'Efforts to construct new and better cyber[security] norms must start by accommodating or at least recognising the existing contexts in which norms are sought', which also includes contexts and processes shaped by non-state actors, which so far have not received extensive scholarly examination.[224] Social science research of the sorts conducted as part of this manuscript, 'can be helpful in understanding what [norm creation] processes ... look like and how they work', as well as who is involved in them and addressed.[225]

2.3 Non-State Actors

Contrary to what the comparatively limited numbers of publications relating to non-state actors in the context of ICTs and security would lead to suggest, the latter have been, and continue to be, central to the evolution of modern cyberspace. As owners and operators of critical systems and network infrastructures, non-state actors have made important contributions to the design and administration of the virtual realm.[226] Furthermore, as investigators of criminal online activities, botnet remediators, and network observers, they have executed important security-related functions.[227]

---

223 Finnemore and Hollis maintained that '[t]he success of a norm rests not just in what it says, but in who accepts it, not to mention where, when, and how they do so. It matters to the content and future of a norm, for example, whether it is promulgated by states at the United Nations, technologists in an industry association, privacy activists in a non-governmental organisation (NGO), or some freestanding multistakeholder group open to all these actors', see Finnemore and Hollis (n 45) 427.

224 Ibid 427.

225 Ibid 477.

226 Laura DeNardis, *The Emerging Field of Internet Governance* (techspace rep, Yale University 2010) ⟨https://perma.cc/Z8VD-7JRZ⟩; Radu (n 35).

227 Kristen E Eichensehr, 'Public-Private Cybersecurity' (2017) 95(467) Texas Law Review 16 ⟨https://perma.cc/ZL8H-48JE⟩; Matt Olsen, Bruce Schneier, and Jonathan Zittrain, *Don't Panic* (techspace rep, Berkman Klein Center for Internet & Society 2016) ⟨https://perma.cc/4ZFT-55C4⟩; Luca Belli and Jamila Venturini, 'Private Ordering and the Rise of Terms of Service as Cyber-Regulation' (2016) 5(4) Internet Policy Review 1 ⟨https://perma.cc/YM44-VW2G⟩.

Conceptually, the advent of non-state actors as providers of global (cyber)security has presented traditionally state-centric scholarly disciplines including international relations and international law, with formidable theoretical and practical challenges and has added new layers of complexity to these subjects. However, '[p]recisely because non-state actors in international security pose a number of serious methodological problems, they constitute an exceptionally instructive field of research'.[228] In order to better comprehend how change occurs in the virtual realm, it is necessary to 'unpack the different categories of transnational actors and understand the quite different logic and processes in these different categories'.[229]

2.3.1 Challenging Traditional Conceptual Confines

While by now, the presence and participation of non-state actors in global policy-making processes have been widely recognised, their roles and status, and even their characteristic features remain greatly contested.[230] Akin to the concepts of *cyberspace* and *cybersecurity* introduced earlier (please refer to the definitional remarks in Section 2.1.1), there are many competing definitions relating to non-state actors. In the broadest sense, non-state actors have been characterised as all actors other than states. Arts, for instance, described non-state actors as 'all those actors that are not (representatives of) states, yet that operate at the international level and are potentially

---

[228] Andreas Kruck and Andrea Schneiker, *Researching Non-State Actors in International Security: Theory and Practice* (Routledge Critical Security Studies, Routledge 2017) 5.

[229] Margaret E Keck and Kathryn Sikkink, 'Transnational Advocacy Networks in International and Regional Politics' (1999) 51(159) International Social Science Journal 89 ⟨https://perma.cc/FR9H-ZFBR⟩, 99.

[230] Andrew Clapham, 'Non-State Actors' in *International Human Rights Law* (April, Oxford University Press 2013) ⟨https://perma.cc/B8JZ-6VND⟩; Allison Peters, Closing the Global Cyber Enforcement Gap (2018) ⟨https://perma.cc/AHB2-CWVA⟩ accessed 19 December 2018; Weissbrodt (n 47); Noortmann and Ryngaert (n 38); Philip Alston, *Non-State Actors and Human Rights* (Collected Courses of the Academy of European Law, Oxford University Press 2005); Math Noortmann, August Reinisch, and Cedric Ryngaert, *Non-State Actors in International Law* (Math Noortmann, August Reinisch, and Cedric Ryngaert eds, Studies in International Law, Hart Publishing 2015).

relevant to international relations'.[231] Following similar tracks, Clapham considered non-state actors to be all non-governmental protagonists belonging to one of the following categories: armed groups, terrorists, civil society, religious groups, corporations, and (occasionally) intergovernmental organisations.[232] Although attractive in terms of definitional simplicity and useful apropos highlighting that '[f]rom both a conceptual as well as an analytical perspective, non-state actors do not match the traditional unit of assessment of international law and international relations', these binary/enumerative understandings of non-state actors are prone to reinforce misleading dichotomies (states as the main objects of reference), and are of limited practical value.[233]

Questioning traditional positivist approaches to international legal personhood, which regard states as the most important (or even only) subjects of international law bearing rights and duties, and non-state actors as objects, Rosalyn Higgins convincingly argued that 'the whole notion of *subjects* and *objects* has no credible reality, and, ... no functional purpose. [International legal scholars] have erected an intellectual prison of [their] own choosing and then declared it to be an unalterable constraint'.[234] Considering international law not to be fixed sets of rules but rather responsive norms reflecting systemic needs, Higgins reasoned for more participatory conceptions of non-state actors, and related international legal doctrines.[235]

---

[231] Bas Arts, 'Non-State Actors in Global Governance: Three Faces of Power' (2003) ⟨https://perma.cc/9TF3-F9VU⟩ 5.

[232] Clapham (n 230).

[233] Math Noortmann, Cedric Ryngaert, and August Reinisch, 'Introduction' in *Non-State Actors in International Law* (Hart Publishing 2015) ⟨https://perma.cc/3CLG-ZNM5⟩ 2.

[234] Rosalyn Higgins, *International Law and How We Use It* (Oxford University Press 1995) ⟨https://perma.cc/C29A-MDLF⟩ 49.

[235] Specifically, Higgins contended that 'it is not particularly helpful, either intellectually or operationally, to rely on the subject-object dichotomy that runs through so much of the writings. It is more helpful, and closer to perceived reality, to return to the view of international law as a particular decision-making process. Within that process (which is a dynamic and not a static one) there are a variety of participants, making claims across state lines, with the object of maximising various values. Determinations will be made on those claims by various authoritative decision makers — Foreign Office Legal Advisers, arbitral tribunals, courts. Now, in this model, there are

Alston, too, criticised the negative lines of conceptual thinking pertaining to non-state actors, and maintained that 'defining all actors in terms of what they are not' is misleading and marginalising.[236] Furthermore, he reasoned that

> these negative, euphemistic terms do not stem from language inadequacies but instead have been intentionally adopted in order to reinforce the assumption that the state is not only the central actor, but also the indispensable and pivotal one around which all other entities revolve.[237]

Rather than advancing counter-definitions, however, Alston identified some of the key factors which had allowed non-state actors to gain a stronger foothold on the global stage, including privatisation, capital mobilisation and private foreign investment flows, trade liberalisation, the expanding scope of multilateral institutions, surging civil society activities, the privatisation of security, as well as the changing nature of conflicts.[238]

Contrary to the broad notions advanced by Arts and Clapham, some experts put forward more context-based understandings of non-state actors. Busé, for instance, argued that non-state actors are synonymous with 'rebel groups, irregular armed groups, insurgents, dissident armed forces, guerrillas, liberation movements, freedom fighters and de facto territorial governing bodies'.[239] While narrow approaches, such as proposed by Busé, hold value in particular circumstances (e.g. in contexts of landmines or arms control regimes), they are of limited use for more general determinations.

---

no *subjects* and *objects*, but only participants. Individuals are participants, along with states, international organisations (such as the United Nations, or the International Monetary Fund (IMF) or the ILO), multinational corporations, and indeed private non-governmental groups', see ibid 50. In the context of cybersecurity governance, and the roles of non-state actors in particular, participatory philosophies appear to be better suited for examining normative structures than traditional positivist understandings.

236 Alston (n 230) 3.

237 Ibid 3.

238 Ibid.

239 Margaret S Busé, 'Non-State Actors and Their Significance' (2001) 5(3) Journal of Mine Action ⟨https://perma.cc/CXL3-LYRS⟩.

To adequately respond to the diversity of non-state actors and pay due regard to their different contexts of emergence as well as agendas, this thesis relies on a redacted version of Josselin's and Wallace's characterisation of non-state actors. It considers non-state actors to include entities, which are

> largely or entirely autonomous from [state control and influence, originating from market forces, civil society, or political impulses outside immediate government direction]; operating as or participating in networks which extend across the boundaries of two or more states – thus engaging in transnational relations, linking political systems, economies, societies; acting in ways which (seek to) affect political outcomes, either within one or more states or within international institutions – either purposefully or semi-purposefully, either as primary objective or as one aspect of their activities.[240]

While still fairly comprehensive in terms of conceptual scope and material quality, above-mentioned definition of non-state actors is more restrictive than characterisations which consider non-state actors to be all actors other than states, and better suited to respond to the practical intricacies concerning non-state entities (for example, the definition captures more than just non-governmental organisations (NGOs)). Given the empirical diversity of non-state actors, it is advisable to adopt a broad approach which is able to include agents pursuing economic goals, such as corporations and trade associations, organisations advocating for principled ideas, including civil society organisations (CSOs), as well as specialists and pundits driven by professional experiences and commitment to well-founded examinations of empirical facts, for instance think-tanks and expert communities.[241] The definition consciously excludes intergovernmental organisations (IGOs), which, for the purposes of this dissertation, are not regarded as non-state agents, as they are primary surrogates of governmental

---

[240] Daphne Josselin and William Wallace, *Non-State Actors in World Politics* (Daphné Josselin and William Wallace eds, Palgrave Macmillan UK 2001) ⟨https://perma.cc/9KGG-VZ6A⟩ 3-4.

[241] Markus Wagner, 'Non-State Actors' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2009) ⟨https://perma.cc/H4JV-SWDB⟩; Josselin and Wallace (n 240).

actors. Although considered by some to constitute (political) protagonists in their own rights, and said to enjoy certain degrees of independence from their member states, their agency and financial potency are chiefly determined by governments.[242]

The definition also takes into account that while often presented as opposing categories, the lines between governmental and non-governmental actors are not always clear-cut. Relationships between governmental and non-governmental actors are often complex, multilayered and impure. For example, '[g]overnments of liberal states [often] provide financial support for some transnational groups, primarily those working in economic and social development. Think-tanks and elite networks often have close links with governments, from funding to participation by officials'.[243] Furthermore, public actors frequently employ and draw on the capabilities of private entities for the provision of services as part of so-called public-private-partnerships (PPPs).[244]

2.3.2 Stirring Up Norm Creation Processes

Despite the emergence of burgeoning scholarly literatures relating to non-state actors across the disciplines of international relations and international law, there remains ample scope for descriptive and analytical accounts pertaining to the roles assumed by non-state actors in global rule- and norm-making processes, particularly in the field of cybersecurity.[245] Mainstream theories of international law and international

---

242 Bob Reinalda, 'Non-State Actors in the International System of States' in *The Ashgate Research Companion to Non-State Actors* (Routledge 2016); Noortmann, Reinisch, and Ryngaert (n 230); Craig Calhoun, *Dictionary of the Social Sciences* (Craig Calhoun ed, October, Oxford University Press 2002) ⟨https://perma.cc/2R32-TBBY⟩.

243 Josselin and Wallace (n 240) 3.

244 Myriam Dunn Cavelty and Manuel Suter, 'Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection' (2009) 2(4) International Journal of Critical Infrastructure Protection 179 ⟨https://perma.cc/KK4N-R2SP⟩; Madeline Carr, 'Public-Private Partnerships in National Cybersecurity Strategies' (2016) 92(1) International Affairs 43 ⟨https://perma.cc/KJ8J-EW6J⟩.

245 Noortmann and Ryngaert (n 38); Peter J Spiro, 'Nongovernmental Organizations in International Relations (Theory)' in Jeffrey L Dunoff and Mark A Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations* (Cambridge University Press 2012).

relations have engaged rather ambivalently with non-state actors. While positivist, realist, and liberal accounts have taken note of non-state actors as empirical entities, their state-centred ontologies have effectively reinforced conceptual and theoretical marginalisations of non-governmental agents. Even constructivist strands, in their pursuit for mainstream acceptance, have underscored the dominant positions of states in global decision and norm-making processes.[246]

Scholars studying interactions and exchanges at the global level through realist lenses have primarily focused their attention on inter-state relations and major power interactions rather than on puzzles surrounding non-state actors.[247] Conditions of anarchy and material capabilities were the key drivers behind realist research programmes.[248] As a result, non-state actors and their participation in global dealings were mostly viewed as epiphenomenal occurrences.[249] If private actors figured as part of realist analyses at all, they were studied as potential intervening variables in explaining courses of action undertaken by states.[250]

Keohane's and Nye's 1977 publication entitled *Power and Independence* served as an early (neo-liberal) push towards less material understandings of political interactions at the global level.[251] Challenging traditional realist doctrines, Keohane and Nye identified

---

246 Math Noortmann, 'Understanding Non-State Actors in the Contemporary World Society: Transcending the International, Mainstreaming the Transnational, or Bringing the Participants Back In?' in Cedric Ryngaert and Math Noortmann (eds), *Non-State Actor Dynamics in International Law* (Routledge 2016) ⟨https://perma.cc/S825-KPCZ⟩.

247 Evan Laksmana, Realism and Non-State Actors Revisited (2013) ⟨https://perma.cc/2NN9-N3G6⟩ accessed 16 July 2019; International Relations, 'Conversations in International Relations: Interview with John J. Mearsheimer (Part II)' (2006) 20(2) International Relations 231 ⟨https://perma.cc/9F8G-BGDG⟩.

248 Anne-Marie Slaughter, 'International Law and International Relations Theory: Twenty Years Later' in Jeffrey L Dunoff and Mark A Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (2012).

249 John J Mearsheimer, 'The False Promise of International Institutions' (1994) 19(3) International Security 5 ⟨https://perma.cc/3K2C-PB4S⟩.

250 Realism and Non-State Actors Revisited (n 247).

251 Robert O Keohane and Joseph SJr Nye, *Power and Independence* (Little, Brown and Company 1977).

different patterns of cooperation and conditions of complex interdependence among state and as non-state actors (mitigating conditions of anarchy, which inspired realist policies of self-help and power competition among governments). It was not until the end of the Cold War, however, that non-state actors became more firmly embedded in the research agendas of international relations scholars and international lawyers. Following the collapse of the Soviet Union, research on non-state actors started to gain traction. 'It first provoked social and political scientists and later international law scholars to engage in what was considered to be a new transnational reality'.[252]

Scholars of liberalism have attributed greater theoretical standing to non-state actors. They have integrated non-state actors in their analytical conceptions and treated non-state actors as relevant entities in the formation of state preferences. Positing that state-society relations, i.e. the domestic and transnational social contexts governmental actors are embedded in meaningfully structure the behaviour of states 'by influencing the social purposes underlying [their] preferences', researchers subscribing to liberal theories have claimed that (a) the demands of private individuals and groups precede politics, that (b) states represent social institutions subject to constant capture and recapture by alliances of social actors, and that (c) the conduct of governments internationally is a function of interdependent state preferences.[253] In contrast to realist conceptions, liberal scholars did not regard states as mere '*black boxes* seeking to survive and prosper in an anarchic system'.[254] Rather, they considered states to be 'configurations of individual and group interests who then project those interests [internationally] through a particular kind of government'.[255]

---

252 Noortmann (n 246) 142.

253 Andrew Moravcsik, 'Taking Preferences Seriously: A Liberal Theory of International Politics' (1997) 51(4) International Organization 513 ⟨https://perma.cc/J8W8-6ZRL⟩, 516.

254 Anne-Marie Slaughter, 'International Relations, Principal Theories' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2011) 4.

255 ibid 4. Slaughter went on to argue that while survival may well rank among those interests, other aspects, including commercial goals or ideological beliefs may be of equal relevance.

Constructivist thinkers have conceptualised non-state actors as crucial cogs in transnational norm development efforts.[256] Underscoring the significance of social artefacts and ideas (ideational factors rather than material capabilities or rational doctrines) pertaining to interactions at the global level, they contended that key facets of politics are socially constructed in the sense that they are outcomes of mutually constitutive processes of interactions between agents and 'the structures of their broader environment'.[257] Whereas neorealists considered systemic structures to be determined mainly by distributions of material capabilities, constructivists have countervailingly argued that they are 'also made of social relationships' which are themselves constructed by three elements of 'shared knowledge, material resources and practices'.[258]

Incorporating constructivist features, transnational legal process frameworks (as opposed to traditional positivist approaches) have underscored the involvement of private agents in promoting global norms and compliance, and offered more plastic understandings of international law than traditional positivist approaches.[259] Although references to non-state actors have increased since the late 1990s, and neo-transnationalist terminologies have gradually found their way into the languages of international law and international relations, they have not (yet) 'resulted in a paradigmatic reconsideration of non-state entities in mainstream thinking'.[260] Insofar

256 Hoffmann (n 43).

257 Jeffrey T Checkel, 'Constructivism and Foreign Policy' in Steve Smith, Amelia Hadfield, and Timothy Dunne (eds), *Foreign Policy: Theories, Actors, Cases* (Oxford University Press 2008) 72. See also Kratochwil and Ruggie (n 177); Onuf (n 177); Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations' (n 77); Wendt, 'The Agent-Structure Problem in International Relations Theory' (n 177); Alexander Wendt, 'Anarchy Is What States Make of It' (1992) 46(2) International Organization 391 ⟨https://perma.cc/V3WX-UCJR⟩.

258 Maysam Behravesh, Constructivism: An Introduction (2011) ⟨https://perma.cc/V9RL-CGL4⟩ accessed 9 February 2018; Alexander Wendt, 'Constructing International Politics' (1995) 20(1) International Security 71 ⟨https://perma.cc/C8HE-SS93⟩.

259 Brunnée and Toope (n 174); Spiro (n 245); Bianchi (n 77).

260 Noortmann (n 246) 142. See also Bianchi (n 77); Thomas Risse-Kappen, *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures and International Institutions* (Cambridge Studies in International Relations, Cambridge University Press 1995). Noortmann argued that contemporary legal research continues to consider non-state agents mainly as 'special cases, selected anomalies, controversial candidatures or *Sonderfälle*', see Noortmann (n 246) 2.

as international legal experts and international relations scholars have endeavoured to theorise about non-state actors and their undertakings at the global level, they have chiefly done so in relation to sovereign entities. And while they have come to appreciate that non-state actors have taken on different roles in global policy-making endeavours, from advocacy agents to capacity builders, and policy implementers, they have often paid little attention to the consequentialities of non-state actor engagement 'not directly implicating state[s]'.[261]

In the context of cybersecurity, calls for more systematic empirical contributions concerning the places of non-state actors in international law- and global decision-making processes have been answered somewhat haphazardly. The modest numbers of political and legal publications relating to non-state actors and cybersecurity have predominantly focused on nefarious private entities, including but not limited to, script-kiddies, (cyber)terrorists, hacker groups (including fairly eclectic cases such as Anonymous), and proxy-actors.[262] Applegate, for instance, looked at the status of political hackers and cybermercenaries in the broader context of conflictual interactions in cyberspace. Referencing the 2007 and 2008 cyberattacks on Estonia and Georgia respectively, he argued that in the virtual realm, applying conventional legal classifications and considerations of distinction to political hackers is extremely difficult, and reviewed the advantages and disadvantages of governments employing hacktivists for achieving offensive objectives in the digital domain. He put forward that against the background of considerable levels of legal ambiguity surrounding malicious behaviour in cyberspace (e.g. when do nefarious cyberactivities amount to acts of war? How can principles of distinction and proportionality be applied? Are

---

[261] Spiro (n 245) 223.

[262] David P Fidler, Russell Buchan, and Emily Crawford, *Study Group Report* (techspace rep, International Law Association 2016) ⟨https://perma.cc/3GQC-59YZ⟩; E Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso 2014); Tim Maurer, *Cyber Mercenaries* (Cambridge University Press 2018).

culprits to be treated as combatants?), states stand to benefit from covertly employing cybermilitias for executing offensive strategies and pursuing political goals. Specifically, Applegate stated that '[a]s long as nations can utilise these types of irregular forces to achieve their objectives with little or no recrimination, these methods will remain an attractive alternative to the use of conventional forces'.[263]

Schmitt and Vihul, in their publication entitled *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, reached similar conclusions. Examining the legal specificities pertaining to proxy-led cyberoperations, they held that it seems inevitable that 'states will continue to work through non-state actors to achieve national security and foreign policy objectives ... for such operations afford states a degree of anonymity and detachment from ... non-state operations that serve useful political and legal ends'.[264] They maintained, however, that pursuant to the Draft Articles on Responsibility of States for Internationally Wrongful Acts, as adopted by the International Law Commission at its 53rd session in 2001 (and annexed to General Assembly resolution 56/83 of 12 December 2001), governments can be called to account for carrying out offensive cyberoperations by means of proxy-actors.[265] If states are found to have exercised effective control or direct instruction over cyberoperations, they can be held responsible for the nefarious activities conducted by non-state actors on their behalves. For that to occur though, the levels of direct control and influence have to be readily discernible and of considerable extent, i.e. simple provision of hard- and software to or financing of proxy-agents would not be sufficient to count as effective control.[266]

---

263 Scott Applegate, 'Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare' (2011) 9(5) IEEE Security & Privacy Magazine 16 ⟨https://perma.cc/2LF4-V229⟩, 21.

264 Michael N Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) 1(2) Fletcher Security Review 55 ⟨https://perma.cc/6XZQ-K8M2k⟩, 72.

265 United Nations General Assembly, Responsibility of States for Internationally Wrongful Acts (2002) ⟨https://perma.cc/5TMJ-KA5A⟩ Art. 8.

266 Schmitt and Vihul (n 264).

With the intention of acquiring more detailed insights into the intricacies of proxy-relationships, Maurer examined why and how modern governments employ cybermercenaries to pursue strategic and geopolitical aims.[267] Offering a set of analytical tools, he argued that three different types of proxy-relationships can be distinguished, i.e. (a) delegation, (b) orchestration, (c) and sanctioning, whereby delegation implies the highest, and sanctioning the lowest degrees of control exerted by state parties.[268] Surveying different case studies, he maintained that the nature and type of proxy-relationships depend on how governments understand security implications (i.e. cybersecurity versus information security) and intend to project influence and power in the virtual realm. Proxy-configurations are also determined by how state-and non-state actors have worked together in the past, according to Maurer.[269]

Topically closely related to Maurer's analytical undertakings, Egloff studied the applicability of historical analogies to cybersecurity contexts. Specifically, he examined how analogies to 'mercantile companies, privateers, and pirates between the 16th and 19th century can elucidate the relationship[s] between non-state actors and states in cyber(in-)security', and how the employment of such analogies can inform understandings of cyber(in-)security.[270] Among other things, he found that analogies related to piracy and privateering help investigators better understand how connections and proximities to governments are utilised by perpetrators and defenders. With regard to mercantile companies, he argued that analogies facilitate more granular understandings of how

[267] According to Maurer, a proxy actor in cyberspace is 'an intermediary that conducts or directly contributes to an offensive cyberoperation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect', Maurer, *Cyber Mercenaries* (n 262) 31.

[268] Ibid.

[269] Following Maurer, Washington has (so far) pursued mainly delegation-driven proxy-strategies, whereas Moscow has primarily implemented proxy-approaches centred on sanctioning. The reasons for these different configurations are to be found in the relevant historic environments within which interactions among state and non-state actors have emerged.

[270] Florian J Egloff, 'Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates' (PhD thesis, University of Oxford 2018) ⟨https://perma.cc/WF6S-YTLR⟩ i.

conflictual and 'cooperative ... relations between large technology companies and states influence cyber(in-)security'.[271]

The International Law Association, and its Study Group on Cybersecurity, Terrorism, and International Law, sought to shed light on the legal complexities associated with cyberterrorism and the related advancement of political and ideological agendas.[272] Under the leadership of David P. Fidler, Professor of Law at *Indiana University School of Law*, the work of the group was structured around four main objectives, i.e. to (a) examine current and future threat characteristics pertaining to cyberterrorism, (b) provide definitional clarifications, taking into account relevant international legal provisions and practices, (c) inventory international laws potentially applicable to cyberterrorism, and (d) '[a]ssess whether proactive international legal actions concerning potential acts of cyberterrorism would be worthwhile and feasible'.[273] While noting that the 21st century had not yet witnessed instances of cyberterrorism, the Study Group on Cybersecurity, Terrorism, and International Law concluded that traditional counter-terrorism response, protection, and prevention strategies provide useful frameworks for mapping the international legal issues potentially relevant to terrorist uses of cyberspace, but that further research is required with regard to comprehensively addressing the (legal) intersections between ICTs and terrorism.[274]

Tsagurias inquired whether states could be held responsible for malicious acts carried out by non-state actors, such as ISIS, operating from ungoverned spaces,

271 Ibid i.

272 As part of its mandate, the Study Group on Cybersecurity, Terrorism, and International Law elaborated a working definition of cyberterrorism. As per its final report, '[c]yberterrorism involves acts intentionally committed by any person who uses information and communication technologies unlawfully in ways that cause, or are intended to cause, death or serious bodily injury to persons, substantial damage to public or private property, the economy, or the environment, or serious disruption of public services and that are undertaken with the intent to spread fear in civilian populations or to compel a government, a civilian population, or an international organisation to take or abstain from specific acts or courses of action', Fidler, Buchan, and Crawford (n 262) 25.

273 Ibid 2.

274 Ibid.

i.e. territories seized by ISIS, e.g. in Syria or Iraq. Identifying responsibility deficits relating to non-state actors operating from ungoverned spaces, he suggested holding non-state actors which exercise effective control over populations and territories directly accountable for their nefarious undertakings (akin to states). Establishing and determining *effectiveness*, however, is difficult and tedious, which is why Tsagurias concluded that 'unless international law engages in a radical conceptual, institutional and structural rebooting, the place, role and consequences of non-state actors and of their acts will remain uncertain'.[275]

Without denying the analytical value of the studies outlined above, this thesis seeks to tread different paths. Rather than studying the implications and characteristics of agents seeking to undermine the security of cyberspace, it wants to examine the consequentialities and contributions of private agents to global cybersecurity norm-making processes, i.e. the contributions of actors striving to strengthen the stability of the digital domain (rather than weaken it). In addition, and more generally, it wants to respond to the modest stocks of research on non-state actors in cybersecurity. International law and international relations can no longer be studied 'in a business-as-usual mode of investigation, when it comes to the appreciation of non-state actors' presence in the international realm'.[276] While not disputing the significance of public actors in shaping and enacting rules of the road for the digital domain, this monograph argues that focusing on public entities alone only provides a partial picture of the forces at work in global steering and norm creation efforts, and that the types and implications of non-state actor activities merit further investigation. As disciplines concerned with dealings at the global level, the default positions of agnosticism of international law and international relations towards the consequentialities of normative endeavours conducted by non-state actors deserve to be further challenged.

---

[275] Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (n 45) 19.

[276] Noortmann, Ryngaert, and Reinisch (n 233) 3.

2.4 Summary

The goal of this chapter was to introduce key literatures and concepts relating to non-state actor-driven cybersecurity norm formation endeavours. Reviewing scholarly works in the areas of international relations and international law, it has developed several working definitions of key concepts, which are summarised in Table 2.1.

This chapter has argued that although recognised as entities under international law and international relations, in the context of cybersecurity, non-state actors have not yet received extensive scholarly treatment apropos their contributions to global governance arrangements. In light of increasing levels of urgency surrounding efforts directed at responding to abuses of information and communication technologies, there is a pressing need for scholarly explorations addressing questions of normative capital and influence.[277]

The next chapter introduces the ontological and epistemological premises of this study and comments on the means and methods of data collection and analysis employed (see *Chapter 3* Methodology and Data). It specifies the sampling tactics used to select the nine case studies, and presents the structural skeleton underlying each of the empirical examples (background, mandate and goals, activities, role profiles, effectiveness review, précis). In addition, it familiarises readers with the analytical frameworks devised to acquire richer understandings about how and in which capacities non-state actors participate in global cybersecurity steering efforts, and how effectively they go about it.

---

[277] Finnemore and Hollis (n 45); Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (n 45); Sigholm (n 45); Buchan (n 45).

Working Definitions	
Cyberspace	Cyberspace denotes 'all computer systems and networks in existence, including air-gapped systems', see Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (2013) 38(2) International Security 7 ⟨https://perma.cc/2CSB-58RZ⟩, 17. In addition to the internet which consists of all interconnected computing devices, including the World Wide Web, cyberspace also comprises the entirety of secluded systems, which are not logically connected to the internet or the World Wide Web.
Cybersecurity	Cybersecurity refers to 'a multifaceted set of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorised access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information', see Myriam Dunn Cavelty, 'Cyber-Security and Private Actors' in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies* (Routledge 2015) ⟨https://perma.cc/Y47N-DWUE⟩ 89.
Non-State Actors	Non-state actors are entities which are 'largely or entirely autonomous from [state control and influence, originating from market forces, civil society, or political impulses outside immediate government direction]; operating as or participating in networks which extend across the boundaries of two or more states – thus engaging in transnational relations, linking political systems, economies, societies; acting in ways which (seek to) affect political outcomes, either within one or more states or within international institutions – either purposefully or semi-purposefully, either as primary objective or as one aspect of their activities', see Daphne Josselin and William Wallace, *Non-State Actors in World Politics* (Daphné Josselin and William Wallace eds, Palgrave Macmillan UK 2001) ⟨https://perma.cc/9KGG-VZ6A⟩ 3-4.
Norms	Norms constitute 'collective expectations for the proper behaviour of actors with a given identity', see Peter J Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press 1996) 5.
Cybersecurity norms	Cybersecurity norms are collective expectations of appropriate behaviour vis-à-vis maintaining global security and stability of cyberspace.

Table 2.1: Summary of Working Definitions.

Norms may also generate or constitute new actors, social facts, and organisational structures. They can vary in their degree of internalisation and draw their propriety or normative force from a wide variety of contexts and cultures, including (but not limited to) law. Like the varying contexts implicating cybersecurity, efforts to construct new cybernorms must account for this normative heterogeneity. At the same time, however, to be successful such efforts must also understand the processes by which norms arise and shape behaviour in the first place.

— Martha Finnemore & Duncan B Hollis,
Constructing Norms for Global Cybersecurity (2016)

3

Methodology, Data, and Analytical Tools

Contents

This chapter provides readers with an overview of the research approach and methods used as part of this scholarly undertaking. With reference to the research design components delineated by Denzin and Lincoln, this chapter begins with brief remarks on the underlying ontological and epistemological premises of this study, and goes on to comment on the data collection and analysis strategies employed, including the sampling tactics used to select relevant case studies. It then introduces the analytical toolkits developed and harnessed as part of this thesis, and concludes with notes on the limitations pertaining to the scientific undertaking at hand.[278]

[278] Norman K Denzin and Yvonna S Lincoln, *Strategies of Qualitative Inquiry* (SAGE Publications 2012). 'Denzin and Lincoln suggested that four basic issues structure the design of a research study: (a) Which paradigm or worldview will inform the study design? (b) Who or what will be studied? (c) Which research strategies will be used? ... (d) Which research methods or tools will be used to collect and analyse data?', see Yilmaz (n 63) 312.

Scholarly endeavours seeking to answer questions of *why* and *how*, as is the case with this investigation, stand to benefit from qualitative approaches.[279] The latter differ from quantitative approaches in that '[t]echnically, a *qualitative observation* identifies the presence or absence of something, in contrast to [a] *quantitative observation*, which involves [determining] the degree to which some feature is present'.[280] Rather than deriving statistical measurements, qualitative approaches are geared towards capturing and categorising 'social phenomena and their meanings'.[281] As Bauer and Gaskell have convincingly stated,

> [o]ne needs to have a notion of qualitative distinctions between social categories before one can measure how many people belong to one or the other category. If one wants to know the colour distribution in a field of flowers, one first needs to establish the set of colours that are in the field; then one can start counting the flowers of a particular colour. The same is true for social facts.[282]

Given the goal of this thesis to better understand how and in which capacities non-state actors contribute to global norm construction efforts pertaining to responsible behaviour in cyberspace, the use of qualitative research frames is well-suited.

In terms of research approach, this manuscript draws on insights from bodies of work in the areas of international relations and international law. By way of combining these disciplines, it is possible to examine global norm construction processes from various angles, and to bring together different analytical elements pertaining to international regulation and governance. With a view to generating deep understandings of 'the

---

279 Greg Guest, Emily E Namey, and Marilyn L Mithcell, 'Qualitative Research: Defining and Designing' in *Collecting Qualitative Data: A Field Manual for Applied Research* (SAGE Publications 2013) ⟨https://perma.cc/W5NS-W8ZV⟩.

280 Lisa Webley, 'Qualitative Approaches to Empirical Legal Research' in Peter Cane and Herbert M Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010) ⟨https://perma.cc/J5AJ-D5H2⟩ 927.

281 Ibid 927.

282 Martin Bauer and George Gaskell, *Qualitative Researching with Text, Image and Sound* (Martin W Bauer and George D Gaskell eds, SAGE Publications Ltd 2000) 9.

makings and unmakings of normativities in global politics' and cybersecurity steering ventures, respectively, uniting non-state actor-focused constructivist (international relations) and neo-transnationalist (international law) lines of thinking in a cross-disciplinary fashion is advantageous.[283]

3.1 Ontology and Epistemology

Congruent with the employment of qualitative approaches, the research design of this thesis is underpinned by relativist ontological and interpretivist/constructivist epistemological assumptions.[284] Contrary to (post-)positivist beliefs, interpretivist paradigms presume multiple social realities (as opposed to one objective reality), which are moulded by human experiences and social contexts.[285] Consequently, in conducting investigations, inductive processes of sense-making take precedence over endeavours of hypothesis testing.[286] As part of their examinations, researchers guided by interpretivist paradigms are receptive to discovering different meanings and generating understandings.[287] Researchers and contexts are thereby mutually constitutive and

[283] Kornprobst (n 47) 321.

[284] Relativist assumptions revolve around 'the belief that reality is a finite subjective experience and nothing exists outside of our thoughts. Reality from a relativist perspective is not distinguishable from the subjective experience of it. ... In this way of thinking, reality is human experience and human experience is reality', see Merry-Jo D Levers, 'Philosophical Paradigms, Grounded Theory, and Perspectives on Emergence' (2013) 3(4) SAGE Open ⟨https://perma.cc/8894-8MAW⟩, 2. Interpretivist paradigms include 'consideration[s] of multiple realities, different actors' perspectives, researcher involvement, taking account of the contexts of the phenomena under study, and the contextual understanding and interpretation of data', see Contributors David Carson and others, 'Philosophy of Research' in *Qualitative Marketing Research* (SAGE Publications, Ltd 2001) 5.

[285] Adherents of positivism presume an objective reality, which exists 'independently of consciousness', and which, given the right analytical tools, can be accurately portrayed, see David E Grey, *Doing Research in the Real World* (SAGE Publications 2018) ⟨http://perma.cc/Y6PG-VCHY⟩; Guest, Namey, and Mithcell (n 279). Post-positivists take a more moderate stance and 'are prepared to admit and deal with imperfections in a phenomenologically messy and methodologically imperfect world, but still believe that objectivity is worth striving for', see Patton (n 64) 93.

[286] Interpretive Research (n 61).

[287] Grey (n 285).

interact. Interpretivist researchers may hold previously acquired notions about relevant research contexts but remain open to and actively engage in discovering new insights.[288]

In going about conducting their examinations, scholars subscribing to interpretivist notions do not follow 'the rigidities of positivism in relation to certain types of problems in the social field[s]'.[289] Rather than trying to isolate 'causal relationships by means of objective facts' and probabilistic evaluations, interpretivist scholars rely on 'more personal process[es]' for gaining insights about their research subjects.[290] Drawing on 'philosophical ideas in phenomenology, symbolic interactionism, hermeneutics', interpretivist approaches underscore elements of *quality* rather than *quantity*.[291]

As opposed to undertakings concerned with theory-testing, interpretivist models are oriented towards framework-building. Ventures concerned with framework generation follow inductive logics, where data in the form of empirical observations drive the construction of concepts and explanations about the phenomena under investigation.[292] For instance, with regard to the study at hand, initial empirical observations of heightened degrees of non-state actor activities pertaining to cybersecurity norm construction motivated and informed further research concerning the contributions made and particular roles taken on by these actors. Analytical insights are the results of inductive research approaches.

---

288 Carson and others (n 284).

289 Ibid 6.

290 Ibid 6.

291 Yilmaz (n 63) 312. Supporters of interpretivist paradigms have argued that 'the scientific method is reductionist and often misses the point of qualitative research [endeavours]', see Guest, Namey, and Mithcell (n 279) 6.

292 Carson and others (n 284).

3.2 Data Collection and Analysis

Interpretivist research projects typically employ naturalistic means and methods of data collection, including, for instance, observations and interviews. Primary and secondary textual data also constitute important elements of these types of research projects, where meanings tend to emerge towards the end of investigative processes.[293]

> The inductive and flexible nature of qualitative data collection methods offers unique advantages in relation to quantitative inquir[ies]. Probably the biggest advantage is the ability to probe into responses or observations as needed and obtain more detailed descriptions and explanations of experiences, behaviours, and beliefs – this is how ... the why and how questions mentioned at the beginning of this chapter [can be answered].[294]

Qualitative methods of data collection and analysis are also suitable for conducting evaluative projects of the sorts referred to in the second part of the research question formulated in *Chapter 1*.[295] Indeed, qualitative methods constitute critical building blocks for evaluative endeavours because they are able to capture and communicate underlying stories concerning particular phenomena.[296] In finding responses to the research question introduced in *Chapter 1*, this thesis employs different data collection methods, including (a) reviews of secondary academic literatures, case materials, and policy documents collected by means of online desk research, (b) process observations, as well as (c) semi-structured expert interviews with practitioners and scholars acquainted with norm construction projects concerning the digital domain. The use of multiple sources of data, also referred to as data triangulation, allows researchers to elicit additional

---

293 WNewton Suter, 'Qualitative Data, Analysis, and Design' in *Introduction to Educational Research: A Critical Thinking Approach* (SAGE Publications 2014).

294 Guest, Namey, and Mithcell (n 279) 21.

295 The research question formulated in *Chapter 1* was phrased as follows: How and in which capacities do non-state actors contribute to global norm construction efforts pertaining to responsible behaviour in cyberspace, and *how effective is their engagement*?

296 Patton (n 64); Guest, Namey, and Mithcell (n 279) 10.

information, gain deeper phenomenological insights, and explore multiple realities.[297] 'Methodological pluralism strengthens the research findings', yields complementary sets of advantages, and compensates for limitations of partisan approaches, including for instance over-representation of certain views.[298]

Even with academic publications concerning cybersecurity generally and global norm-making efforts specifically increasing in numbers and analytical scope, the roles of non-state actors in cybersecurity steering efforts have remained under-explored. With few exceptions, scholars have not conducted systematic and empirically-grounded analyses of the contributions of non-state actors to norm creation projects concerning the digital domain. Where actor-oriented examinations have been carried out, inquiries have mainly focused on investigating the parts played by states, e.g. across intergovernmental fora such as the United Nations. While these undertakings have generated important yardsticks, they have side-lined analyses relating to actors other than states taking part in global steering and norm creation ventures. By probing more deeply into the normative contributions made by non-governmental actors, this thesis seeks to chart new territories and offer new perspectives on the complexities surrounding global cybersecurity norm formation processes. It also increases the numbers of empirical data points and substantive analyses available relating to these processes.

To comprehend social realities and elucidate phenomenological meanings, qualitative research designs often focus on small, purposefully selected samples of case studies (small-N research). As part of case-oriented undertakings, researchers explore 'real-life, contemporary ... bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of observation (e.g., observations, interviews,

[297] Salkind (n 67); Crowe and others (n 65).

[298] Nasiritousi (n 52) 28.

audiovisual material, and documents and reports), and [report case descriptions] and case themes'.[299]

With a view to identifying and contextualising the roles and contributions of non-state actors to global cybersecurity norm-making processes, this thesis draws on nine strategically selected case studies, belonging to one of the following stakeholder clusters: (a) civil society and academia, (b) corporate actors, and (c) expert communities. The empirical examples selected for analysis include the following entities: (a) Global Partners Digital, (b) the second International Group of Experts (c) the Hague Program for Cyber Norms, (d) Microsoft, (e) Siemens, (f) Kaspersky Lab, (g) the Global Commission on the Stability of Cyberspace, (h) the Forum of Incident Response and Security Teams (FIRST), and (i) Carnegie Endowment for International Peace. Table 3.1 provides an overview of the three stakeholder clusters. All of the cases were purposefully sampled, taking into account factors such as stakeholder affiliation, informativeness, typicality, policy prevalence and relevance, analytical maturity, as well as availability of data and documentation.[300] Informed by the research question, the cases selected exemplify a broad spectrum of different instances of non-state actor norm formation endeavours, and exhibit elements of global reach.

'The logic and power of purposeful sampling lies in selecting information-rich cases for study in depth. Information-rich cases are those from which one can learn a great

---

[299] Creswell (n 60); Nerida Hyett, Amanda Kenny, and Virginia Dickson-Swift, 'Methodology or Method a Critical Review of Qualitative Case Study Reports' (2014) 9(1) International Journal of Qualitative Studies on Health and Well-being ⟨https://perma.cc/AEB6-WL4M⟩, 97. For the purposes of this thesis and in line with Stake, case studies are not seen as data collection tools but as 'choice[s] of what is to be studied', see Robert E Stake, 'Qualitative Case Studies' in Norman K Denzin and Yvonna S Lincoln (eds), *The SAGE Handbook of Qualitative Research* (Sage 2005) 443.

[300] Creswell (n 60); Linda Mabry, 'Case Study in Social Research' in *The SAGE Handbook of Social Research Methods* (SAGE Publications, Ltd 2008). Representative sampling strategies may not have yielded an equally broad or rich spectrum of cases and may not have provided equally comprehensive insights into the contributions of non-state actors to cybersecurity governance projects, see Ben Willis, 'The Advantages and Limitations of Single Case Study Analysis' [2014] E-International Relations 1 ⟨https://perma.cc/KMJ5-MU7V⟩.

Civil Society & Academia	Global Partners Digital Second International Group of Experts The Hague Program for Cyber Norms
Corporate Actors	Microsoft Siemens Kaspersky Lab
Expert Communities	Global Commission on the Stability of Cyberspace FIRST Carnegie Endowment for International Peace

Table 3.1: Overview of Case Studies per Stakeholder Cluster.

deal about issues of central importance to the purpose[s] of the research'.[301] In contrast to randomly selected probability samples, purposefully selected samples offer higher levels of context specificity and empirical depth.[302] While purposefully chosen, the selection of cases does not prejudice the quality of the contributions made by non-state actors to cybersecurity norm formation projects (i.e. the main artefacts under scrutiny) but in fact strengthens aspects of diversity.

The case studies selected for investigation are approached as single cases rather than comparative cases. This does not mean that no comparisons can be made on the bases of the conclusions reached. It does imply, however, that possibilities for inference are limited and generalisations need to be issued with very high degrees of caution.[303] Given the dearth of data pertaining to the roles executed by non-state actors in cybersecurity governance endeavours, the case studies are intended to explore and shed light on the (different) contributions made by these actors. The results obtained by means of these exploratory analyses also inform the effectiveness-oriented evaluations of non-state actor endeavours conducted across *Chapters 4*, *5*, and *6*.

In terms of structure, the nine case studies all follow the same high-level sequence. Each case begins with some contextual remarks, before considering the mandate and

[301] Patton (n 64) 230.

[302] Mabry (n 300).

[303] Webley (n 280); Patton (n 64).

goals of the relevant actors under investigation as well as efforts undertaken in the remit of creating rules of the road for cyberspace. Each case then progresses with examinations of the main roles executed by the relevant actors and effectiveness-oriented assessments of their activities. A brief summary highlighting the main insights acquired concludes each case. Case-oriented investigations typically draw on different means and methods of data collection. In what follows, each data collection method used as part of this scholarly undertaking is elaborated on in more detail. The data collection methods employed as part of this thesis include: (a) reviews of primary and secondary materials, (b) observations, and (c) expert interviews.

3.2.1 Reviews of Primary and Secondary Sources

With the intention of establishing solid theoretical baselines, data comprising more than 600 primary and secondary sources related to the topic and actors under consideration were collected. Search processes followed iterative patterns and relied on both academic and non-academic databases and search engines, including Google Search, Google Scholar, Google Books, Scopus, Web of Science, EBSCO Information Services, Search Oxford Libraries Online, Social Science Research Network, and others. Search terms entered included, among others, non-state actors and cybersecurity, (corporate) norm entrepreneurship, cyber(security) norms, non-state actors and responsible behaviour in cyberspace, private governance and law-making in cyberspace, cybersecurity norm development, non-state actor effectiveness, etc. In addition to these search terms, the names of all nine actors (case studies) as well as their norms-related activities were screened and relevant entries added to the corpus of materials. The types of artefacts gathered included blog posts, website archives, transcripts of speeches, legal acts, policy briefings and reports, guidelines, meeting summaries, statements and

agreements, books, peer-reviewed academic articles, media clippings, technical reports issued by security companies, as well as conference presentations.[304]

Assembling primary as well as secondary (textual) sources allows researchers to triangulate data points and elicit different perspectives. While primary sources such as blog posts or policy reports, provide opportunities for new interpretations and discoveries, secondary sources offer readily accessible (comparative) benchmarks and (peer-reviewed) topical insights.[305] When collecting and analysing documents, however, it is useful to remember that

> [t]hey are written in order to convey an impression, one that will be favourable to the authors and those whom they represent. Moreover, any document should be viewed as linked to other documents, because invariably they refer to and/or are a response to other documents. Other documents form part of the context or background to the writing of a document. Atkinson and Coffey refer to the interconnectedness of documents as intertextuality.[306]

With regard to the examination at hand, text-based analyses provide important entry points for acquiring insights into the roles executed by non-state actors in global cybersecurity governance processes. They allow researchers to gain better understandings of how these actors choose to represent themselves in official texts, or are represented by other observers in terms of the functions they carry out.[307]

3.2.2 Observations

In addition to desk-based reviews of primary and secondary materials, this thesis also relied on and made use of data collected during conferences and public internet

---

[304] To ensure data retrievability post publication, all online data gathered were archived using perma.cc, an archiving tool maintained by the Harvard Law School Library, see Perma cc, About (2020) ⟨https://perma.cc/9WJT-2T7T⟩ accessed 29 January 2020.

[305] Mike Allen, *The SAGE Encyclopedia of Communication Research Methods* (SAGE Publications, Inc 2017).

[306] Bryman (n 69) 555.

[307] Nasiritousi (n 52).

policy meetings. Observational data collection methods are valuable for gathering data in 'natural' settings and minimise 'problems inherent in self-reported accounts'.[308] Furthermore, they can support the development of theory as well as the explanation of social processes pertaining to norm creation in the digital domain.[309]

This thesis benefited from observations undertaken at venues including the United Nations Internet Governance Forum, or the European Dialogue on Internet Governance. Table 3.2 provides an overview of all venues of observation visited. All of the venues listed in Table 3.2 were open to participation from both state and non-state actors (but deliberately encouraged participation from non-state actors) and promoted disciplinary as well as geographical diversity. In addition, they were all concerned (either in part or in full) with questions relating to cybersecurity norm development and discussions surrounding responsible behaviour in cyberspace. Owing to their multistakeholder-oriented setup, all of the venues surveyed, offered rich canvasses for ego- and alter-focused observations.[310]

Apart from high-level observations relating to interactions among state and non-state actors in these international meetings, examinations predominantly focused on questions concerning the contributions of non-state actors to cybersecurity norm-making processes. During the relevant sessions, notes were taken on the roles executed by non-state actors and their effects on discussions pertaining to global cybersecurity governance. The notes compiled were then coded as part of data analysis. The examinations conducted

308 Sonya J Morgan and others, 'Case Study Observational Research: A Framework for Conducting Case Study Research Where Observation Data Are the Focus' (2017) 27(7) Qualitative Health Research 1060 ⟨https://perma.cc/5SPT-XSA6⟩, 1060.

309 ibid. According to Jorgensen, observations are 'especially appropriate for exploratory studies, descriptive studies, and studies aimed at generating theoretical interpretations. Though less useful for testing theories, findings of participant observational research certainly are [also] appropriate for critically examining theories and other claims to knowledge', see Danny L Jorgensen, 'The Methodology of Participant Observation' in *Participant Observation* (SAGE Publications, Inc 1989) 13.

310 All observations were conducted in situ, i.e. as participant of the relevant meetings. The degrees of active participation varied from meeting to meeting.

Year	Location	Venue
2017 2018 2019	Geneva Paris Berlin	United Nations Internet Governance Forum
2018	Geneva	Geneva Dialogue on Responsible Behaviour in Cyberspace
2018 2019	The Hague The Hague	The Hague Program for Cyber Norms Conference
2018 2019	Tbilisi The Hague	European Dialogue on Internet Governance (EuroDIG)

Table 3.2: Venues of Observation.

were largely unstructured and did not follow rigid observational protocols (e.g. such as proposed by Jorgensen in the case of participant observations).[311] This did not prevent the observer from acquiring valuable insights into the practices of cybersecurity norm-making and the dynamics between state and non-state actors, however.[312]

3.2.3 Semi-Structured Expert Interviews

With a view to limiting possibilities for misrepresentation, the empirical data obtained by means of (process) observations were further supplemented by 32 semi-structured interviews with practitioners and scholars acquainted with norm construction projects concerning the digital domain. Semi-structured expert interviews present a systematic and well-defined method of data collection with clear goals and guidelines. Combining the structuredness of survey instruments with the flexibility of open-ended consultations, semi-structured interviews allow researchers to obtain semantic, qualitative data at factor level.[313] With the intention of gaining rich descriptive accounts relating to the

311 Jorgensen (n 309).

312 Nasiritousi (n 52).

313 Stephen L Schensul, Jean J Schensul, and Margaret Diane LeCompte, *Essential Ethnographic Methods: Observations, Interviews, and Questionnaires* (Altamira Press 1999) 149. 'Conducted conversationally with one respondent at a time, [semi-structured interviews employ] a blend of closed- and open-ended questions, often accompanied by follow-up why or how questions.

cases under investigation, interviewees were sampled based on their proximity to and knowledge of the relevant entities and processes under consideration. Factors such as geographical origin, gender, as well as stakeholder group affiliation were also considered. In total, 45 emails were sent out to potential interview partners, of which 32 agreed to partake in the study. Interview dates were arranged with each participant on an individual basis. The final interview sample consisted of participants from North and Latin America, Africa, Europe and Asia-Pacific.

Even though ambitions for diversity in geographical representation were high, the sample ended up being skewed towards Northern American and European viewpoints. The unintended under-representation of voices from the Global South may be emblematic of the comparatively high participation thresholds for actors from these regions. For many protagonists in the Global South, debates about norms of responsible behaviour in cyberspace have been outshone by other (more) pressing governance and infrastructure struggles. Moreover, with a great number of cybersecurity norms-related discussions taking place in the Global North, actors from less capacitated nations 'are often unable to participate in the resource-intensive jet-set diplomacy of the current fragmented processes'.[314] In order not to leave representatives from the Global South behind, and to integrate various viewpoints and realities pertaining to norms of responsible behaviour in cyberspace, streamlining relevant policy processes is critical.

> Building cybersecurity capacity in existing local polities and communities and understanding how these become (trans)formed through their entanglement with global digital connections, international policies and regulations is more important than ever. This calls not only for more research and data collection, but also for better inclusion of developing countries in global

The dialogue can meander around the topics on the agenda – rather than adhering slavishly to verbatim questions as in a standardised survey – and may delve into totally unforeseen issues', see William C Adams, Conducting Semi-Structured Interviews (Wiley Online Books, 2015) ⟨https://perma.cc/S78L-LVUP⟩ 493.

[314] Christian Ruhl and others, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (techspace rep, February, Carnegie Endowment for International Peace 2020) ⟨https://perma.cc/WXC3-JAEP⟩ 15.

> arenas where international norms and global governance on cyberspace are being produced.[315]

The same holds true for non-state actors in the Global South. Indeed, this thesis has identified more concerted examination efforts pertaining to how non-state actors in the Global South contribute to debates about rules of the road for the virtual realm as promising trajectories for further research (please refer to *Chapter 8* for more details).

Prior to engaging in conversations, participants were sent a short synopsis of the research proposal, as well as a copy of the consent form drafted in accordance with university regulations. When requested, interviewees were also sent a copy of the interview guide ahead of the scheduled appointment.[316] The interview guide drafted for this thesis consisted of 14 questions which were adapted (in number and style) to the interviewees' backgrounds. All questions were devised with a view to obtaining data related to the research question formulated in *Chapter 1*, and focused on issues such as non-state actors' underlying motivations for participating in norm creation processes, relevant roles assumed, as well as implementation procedures and appropriate measures of effectiveness applied. Special attention was paid to phrasing open, non-leading questions. Interviews held lasted between 30 and 60 minutes and were conducted over the course of eight months (June 2019-February 2020). When permission for audio-recording was granted, interviews were taped and coded, as well as partially transcribed for direct quotations. Where audio-recording was not permitted, conversation-related notes were taken. With the exception of four interviews which were conducted in person, all of the conversations were done over *Voice over Internet Protocol* (VoIP) services. The language of conversation was English for all of the interviews.

---

315 Niels Nagelhus Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South' (2018) 39(5) Third World Quarterly 821 ⟨https://perma.cc/3UW7-XLM3⟩, 14.

316 A copy of the interview guide was requested six times. Please refer to section 9.2.1 in the *Appendix* for a list of sample questions asked.

Participants were assured anonymity, which is why any responses cited as part of this thesis are referenced with the relevant interviewee number rather than name. It should be noted that the sample is not representative. Participants were deliberately drawn from non-state actor backgrounds. In terms of gender distribution, the number of male participants interviewed (n=22) was twice as high as the number of female candidates surveyed (n=10), even though ambitions for equal distribution were high. With regard to stakeholder affiliation, the majority of interviewees were members of expert communities (n=10), followed by industry delegates (n=9), civil society representatives (n=7), and academics (n=6). An overview of the individuals surveyed, as well as information pertaining to their gender and stakeholder group affiliation can be found in Table 9.1 in the *Appendix*.

The insights gathered from the interviews were aggregated with the data obtained from the observations and the information of the textual sources analysed, and together informed this thesis' understanding of the roles executed by non-state actors in cybersecurity norm formation projects. Given that this thesis was primarily concerned with what respondents 'said rather than how they said it', the absence of nonverbal artefacts resulting from the use of VoIP technologies did not constitute an issue.[317]

3.2.4 Data Analysis

For qualitative research endeavours to yield meaningful and informative results, and be accepted as scientifically rigorous and trustworthy, data-based evaluations have to be done in 'a precise, consistent, and exhaustive manner through recording, systematising, and disclosing the methods of analysis with enough detail to enable [readers] to determine whether the process is credible'.[318] When evaluating information, researchers

[317] Nasiritousi (n 52) 32.

[318] Lorelli S Nowell and others, 'Thematic Analysis' (2017) 16(1) International Journal of Qualitative Methods ⟨https://perma.cc/567A-KUU7⟩, 1.

become key instruments for 'analysis, making judgements about coding, theming, decontextualising, and recontextualising the data'.[319] With regard to the investigation at hand, data analysis was guided by thematic analysis. Thematic analysis denotes a widely employed method used to rigorously and systematically analyse textual data.[320] Thematic analysis allows researchers to uncover, describe, and report patterns or themes within qualitative data, and extract meaning and develop empirical knowledge.[321]

Although widely employed, there is little agreement about how to go about identifying themes.[322] This thesis followed the six-steps approach for detecting patterns in textual data as proposed by Braun and Clarke, as well as Nowell and others.[323] The six steps applied as part of data analysis included: (a) acquiring data familiarity, (b) generating initial codes, (c) searching for themes, (d) reviewing themes, (e) defining and naming themes, and (f) documenting themes (producing written outputs).[324] Data organisation, classification, and evaluation were largely done by hand and in a second step, once codes had been aggregated to initial themes, supported by NVivo, a software package designed for computer-assisted qualitative data analysis.[325]

While the six-steps model for identifying themes in textual raw data would suggest linear progressions from one stage to the next, it is important to acknowledge that when conducting qualitative research, processes pertaining to data collection, data

---

319 Nowell and others (n 318) 2.

320 Wach, Ward, and Jacimovic (n 68).

321 Braun and Clarke (n 70); Bowen (n 69); Bryman (n 69). According to Braun and Clarke, thematic analysis can, among other things, '(a) usefully summarise key features of a large body of data, and/or offer a *thick description* of the data set, (b) ... highlight similarities and differences across the data set, and (c) ... generate unanticipated insights', see Braun and Clarke (n 70) 97.

322 Braun and Clarke (n 70); Anthony G Tuckett, 'Applying Thematic Analysis Theory to Practice: A Researcher's Experience' (2005) 19(1-2) Contemporary Nurse 75 ⟨https://perma.cc/BP3B-HHAC⟩; Jennifer Attride-Stirling, 'Thematic Networks: An Analytic Tool for Qualitative Research' (2001) 1(3) Qualitative Research 385 ⟨https://perma.cc/CG4E-GKYS⟩.

323 Braun and Clarke (n 70); Nowell and others (n 318).

324 Braun and Clarke (n 70).

325 What is NVivo? (n 71).

analysis, and report writing do not always follow linear logics. Rather, the different phases are often interrelated and exhibit iterative, reflective patterns, which require researchers to go back and forth between them.[326] Subsequent to multiple rounds of inductive coding of case study-related materials (interview recordings, observational notes, as well as primary and secondary literatures) the following seven non-state actor-related role profiles (themes) were identified across the nine case studies selected: (a) knowledge brokers, (b) awareness raisers, (c) norm leaders and cooperation incubators, (d) diplomatic change agents, (e) discussion feeders and gap fillers, (f) implementation assistants and capacity builders, and (g) custom shapers.[327]

Data collection and analysis efforts focused on materials produced between 2007 and the first half of 2020. Notwithstanding the introduction of this temporal perimeter, it is important to acknowledge that the empirical and conceptual confines of this research project are inherently transitory and in constant flux. Such being the case, data reliability, validity, and generalisability have to be evaluated within their discrete contexts of emergence.

3.3 Analytical Tools and Frameworks

The previous remarks have underscored that in the remit of cybersecurity, non-state actors have not received extensive scholarly attention apropos their inputs to global regulatory projects. While experts in the fields of international relations and international law, two disciplines that have served as key lenses through which to examine global norm construction and implementation processes, have explored

[326] Nowell and others (n 318). 'Qualitative data analysis is less technical, less prescribed, and less linear but more iterative (back and forth) than quantitative analysis. ... Qualitative data analysis evolves throughout the whole research project and is clearly not summarised by a single number such as a p value, as is the case with quantitative studies, see Suter (n 293) 352.'

[327] The identification of the key themes followed phases of theoretical saturation regarding individual codes (no more new codes would emerge).

the (normative) contributions made by non-governmental organisations (NGOs) and business networks across contexts such as climate change or human rights, they have not conducted analyses of similar breadth and depth across cybersecurity-related issue areas.[328] What is more, 'these non-state actors have been studied [predominantly] for their advocacy activities directed at states and international organisations or in providing expert advice to these traditional governors in world politics rather than as rule-makers and enforcers themselves'.[329]

This thesis seeks to offer analytical correctives and cast wider nets. It is interested in identifying additional roles taken on by non-state actors 'beyond simply acting as pressure or advisory groups lobbying or advising states and international organisations to make or change standards, rules and practices'.[330] In addition to identifying further roles executed by non-state actors, this manuscript seeks to determine the effectiveness of their activities, and study relevant implications for cybersecurity governance arrangements as well as related accountability and legitimacy questions. To facilitate the intended examinations, this thesis relies on two analytical frameworks (please refer to Figure 3.1 and Figure 3.2, respectively), which are specified in further detail below. The conceptual tools developed as part of this thesis help organise and better understand in qualitative terms the roles executed by non-state actors in cybersecurity norm formation ventures. By mapping and dissecting their contributions, these instruments also help reveal new, analytically relevant input categories underlying global governance processes.

---

328 Breslin and Nesadurai (n 44); Naghmeh Nasiritousi, Mattias Hjerpe, and Björn-Ola Linnér, 'The Roles of Non-State Actors in Climate Change Governance: Understanding Agency Through Governance Profiles' (2016) 16(1) International Environmental Agreements: Politics, Law and Economics 109 ⟨https://perma.cc/P4EB-WSFT⟩; Liliana B Andonova, Michele M Betsill, and Harriet Bulkeley, 'Transnational Climate Governance' (2009) 9(2) Global Environmental Politics 52 ⟨https://perma.cc/B8B4-WJKZ⟩; Michele M Betsill and Elisabeth Corell, 'NGO Influence in International Environmental Negotiations: A Framework for Analysis' (2001) 1(4) Global Environmental Politics 65 ⟨https://perma.cc/W2E6-97VX⟩; Keck and Sikkink (n 229).

329 Breslin and Nesadurai (n 44) 190.

330 Ibid 190.

Rather than relying on existing role typologies, which have mostly been developed for categorising NGO activities, this manuscript strives to identify and develop cybersecurity-specific role profiles based on extensive reviews of primary and secondary sources relating to the efforts undertaken by the nine non-state actors under investigation, as well as through semi-structured interviews with subject matter experts, and process observations.[331] To highlight variations in the roles taken on as well as differences in the quality of their activities, this thesis relies on a *non-state actor contributions spectrum*. The latter is a conceptual tool which has been developed as part of this thesis to help plot the different parts assumed by non-state actors in global cybersecurity norm formation processes as well as determine the qualitative characteristics of their contributions (see Figure 3.1).[332] Based on insights from the non-state actor-related scholarly works studied above as well as social movement theories, this thesis distinguishes four different, yet related contribution qualities, namely (a) sensitising, (b) substantive, (c) structural, and (d) procedural characteristics. Grosso modo, the four contribution facets can be distinguished as follows: contributions with sensitising characteristics typically involve elements of agenda-building, awareness-raising, and opinion-influencing. Contributions with substantive qualities show features of policy- and law-making. Procedurally-oriented contributions generally exhibit signs of participation-broadening and access-widening, while structurally-geared contributions

[331] In seeking to understand how and under which conditions NGOs contribute to international negotiations, Albin identified seven types of formal and informal activities executed by NGOs, including: (a) defining problems, setting agendas and goals; (b) enforcing norms and principles; (c) providing knowledge and expertise; (d) engaging in advocacy; (e) lobbying; (f) formulating international agreements, and; (g) assisting with compliance, see Cecilia Albin, 'Can NGOs Enhance the Effectiveness of International Negotiation?' (1999) 4(3) International Negotiation 371 ⟨https://perma.cc/A59H-CUAV⟩. Building on Albin's work, Nasiritousi and others added two further categories, i.e. evaluating consequences of policies, and representing public opinion and marginalised voices, see Nasiritousi, Hjerpe, and Linnér (n 328).

[332] See Jessica Fjeld and others, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI* (techspace rep, Berkman Klein Center for Internet and Society 2020) ⟨https://perma.cc/8FU2-6J2H⟩ for similar visualisations.

include elements of context- and representation-reframing.[333]

Social movement theorists have employed these four contribution categories for evaluating collective action efforts.[334] For the purposes of this manuscript, they are used as qualitative schematisations for characterising different cybersecurity-related non-state actor activities, i.e. they serve as structuring elements. Conceptually, social movement, non-state actor, and norm literatures are fairly closely aligned in that they share common interests in analysing and making sense of ideational efforts undertaken by non-state entities with a view to changing existing frames of reference.

The contributions spectrum as depicted in Figure 3.1 consists of nested concentric circles which reflect different non-state actor roles. Across the circles extend nine beams/rays which represent the different case studies/actors surveyed. The roles executed by the entities under examination are flagged/plotted with either one of four symbols, which indicate the qualitative characteristics of the relevant non-state actor contributions ((a) sensitising, (b) substantive, (c) structural, and (d) procedural).

In addition to providing structures for organisation and clustering, the spectrum helps illuminate qualitative variations concerning the contributions made by non-state actors to cybersecurity norm formation projects. Conceptually, the spectrum is simple, yet comprehensive enough to usefully illustrate these variations. Uniting actors (and stakeholder clusters), contributions, and roles, the spectrum helps reveal distinct patterns of normative inputs and functions assumed.

Apropos determining the success of their undertakings, this thesis draws on legal and regime theoretical insights.[335] The roles played and activities carried out by the nine

---

[333] Hanspeter Kriesi, *New Social Movements in Western Europe: A Comparative Analysis* (University of Minnesota Press 1995).

[334] Kriesi (n 333); Robert F Drake, *The Principles of Social Policy* (Palgrave Macmillan UK 2001).

[335] Yuval Shany, 'Assessing the Effectiveness of International Courts: A Goal-Based Approach' (2012) 106(2) The American Journal of International Law 225 ⟨https://perma.cc/X9YF-MYWT⟩; Hendrik Hegemann, Regina Heller, and Martin Kahl, *Studying 'Effectiveness' in*

Figure 3.1: Example of Non-State Actor Contributions Spectrum.

non-state actors under investigation are assessed along three effectiveness dimensions, i.e. (a) output, (b) outcome, and (c) impact.[336] Even though 'many of the core issues and problems of international politics require answers to ... questions of whether, how, and when certain actors, tools, or policies cause or at least affect specific results', analysing and determining the consequences (positive or negative) of, for example, non-state actor inputs in the remit of global cybersecurity, have remained extremely challenging undertakings.[337] However, conducting performative appraisals is critical

International Relations: A Guide for Students and Scholars (Hendrik Hegemann, Regina Heller, and Martin Kahl eds, Verlag Barbara Budrich 2012); Arild Underdal and Oran R Young, *Regime Consequences: Methodological Challenges and Research Strategies* (Springer Netherlands 2004) ⟨https://perma.cc/8VL6-NYHK⟩.

336 'Effectiveness is a concept defined in varying ways: for example, as the degree to which a rule induces changes in behaviour that further the rule's goals; improves the state of the underlying problem; or achieves its policy objective', see Kal Raustiala and Anne-Marie Slaughter, 'International Law, International Relations and Compliance' in *Handbook of International Relations* (SAGE Publications 2012) ⟨https://perma.cc/G54M-ZTZH⟩ 539.

337 Hegemann, Heller, and Kahl (n 335) 15. With regard to the contributions of non-state actors to

for adequately understanding, and where necessary adjusting, the problem-solving capabilities of the actors engaged in global steering projects, as well as for issuing decisions and value judgements concerning the effects of their efforts.[338] In order to suggest alternatives to dominant courses of action, for instance, it is essential to examine the consequences of governance activities and the degrees to which the latter meet proclaimed goals. Moreover, effectiveness-oriented analyses are also useful for probing, and where applicable correcting, the 'validity of prevalent theoretical assumptions'.[339]

Applying adequate baselines for measuring success involves complicated methodological decisions and trade-offs. In line with studies conducted by Easton, Underdal and Young, Beisheim and others, Flohr and others, Shany, and Wolf, this thesis understands effectiveness to comprise three elements: (a) output, (b) outcome, and (c) impact.[340] The three dimensions can be distinguished as follows: output refers to identifiable commitments and achievements set by actors engaging in global steering efforts.[341] The latter can comprise norms, standards and regulations, programs, as well as institutional structures. Performatively linked to output, outcome, denotes changes in the conduct of participating actors in accordance with the commitments stipulated.[342] Impact relates

---

global cybersecurity steering efforts, key questions, for instance, include: *what counts as success*? Is it raising awareness around issues of considerable urgency, setting action agendas and issuing policy commitments? Is it producing observable outcomes or adding to pools of knowledge and expertise? Or is it fundamentally changing normative terms of reference?

338 Hegemann, Heller, and Kahl (n 335).

339 Ibid 15.

340 David Easton, *A Systems Analysis of Political Life* (Wiley 1965); Underdal and Young (n 335); Flohr and others, *The Role of Business in Global Governance* (n 219); Marianne Beisheim and Andrea Liese, 'Research Design: Measuring and Explaining the Effectiveness of PPPs' in *Transnational Partnerships* (Palgrave Macmillan UK 2014); Shany (n 335); Klaus Dieter Wolf, 'Output, Outcome, Impact: Focusing the Analytical Lens for Evaluating the Success of Corporate Contributions to Peace-Building and Conflict Prevention' (2010) ⟨https://perma.cc/STL2-35UH⟩. Parts of this chapter have been published as Jacqueline Eggenschwiler, 'Expert Commissions and Norms of Responsible Behaviour in Cyberspace: A Review of the Activities of the GCSC' [2020] Digital Policy, Regulation and Governance ⟨https://perma.cc/4QKH-F2WG⟩.

341 Hegemann, Heller, and Kahl (n 335); Beisheim and Liese (n 340).

342 Flohr and others, *The Role of Business in Global Governance* (n 219).

to contributions to problem-solving resulting from the behavioural alterations of the stakeholders involved. While output and outcome facilitate analyses of non-state actor functions, impact enables differentiations between commitments and actions on the one hand and their larger effects on the other.[343] Although analytically separated, the three categories 'are closely connected and may even be regarded as parts of a causal chain'.[344] For instance, actors cannot change the state of global cybersecurity (impact) without first modifying the conduct of state and non-state actors (outcome). However, they may succeed at issuing catalogues of norms of responsible behaviour in cyberspace (output) without enhancing the overall stability and security of the virtual realm (impact).[345]

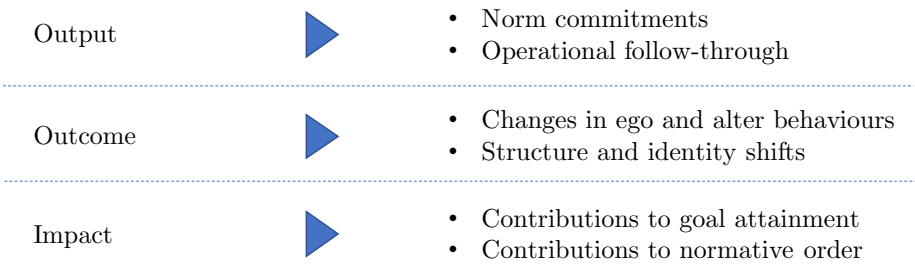

Figure 3.2: Effectiveness Dimensions.

With regard to conducting performative evaluations, assessing output is relatively unproblematic, while determining outcome and impact are analytically more demanding. Especially apropos impact, issues pertaining to data reliability and multi-causality complicate examinations.[346] Furthermore, effectiveness reviews involving non-state actors have frequently been impeded by problems of overestimation/affirmation bias and variations in evaluation baselines, particularly vis-à-vis stated objectives.[347] The

[343] Wolf (n 340).

[344] Ibid 4.

[345] Underdal and Young (n 335).

[346] Wolf (n 340); Hegemann, Heller, and Kahl (n 335).

[347] Referencing Betsill and Correll, Dany maintained that 'there often is discrepancy between what NGOs state publicly and what they actually seek to achieve. ... NGOs frequently seem to put forward extreme positions with the aim of at least achieving a compromise', see Charlotte Dany, 'Between Big Deals and Small Steps: Measuring the Effectiveness of International Non-

results presented in this thesis have to be understood within the contexts of these limitations. However, conscious of these pitfalls, this thesis seeks to limit these caveats by employing a number of mitigation measures, including methods triangulation, as well as process orientation.[348]

Given the contextual complexities concerning the subject matter under investigation, this thesis steers away from assessing effectiveness in quantitative terms and from creating 'false impressions of measurability', and instead evaluates non-state actor contributions to cybersecurity norm-making processes along a three-point ordinal scale (high, medium, and low) across the three effectiveness dimensions.[349] Doing so allows this manuscript to make out variations in effectiveness and identify potential gaps, as well as degrees of politico-legal influence.

To assess the levels of effectiveness yielded, this thesis has developed several benchmark criteria, which are summarised in Table 3.3 per effectiveness category and rating band. The benchmark criteria delineate and help understand relevant evaluation scores (high/medium/low) across the three effectiveness dimensions (e.g. what does a high score across the output dimension mean or imply?). They represent the yardsticks against which the activities of the actors surveyed across *Chapters 4*, *5*, and *6* will be evaluated. Evidence relating to the relevant benchmarks devised is collected from a variety of sources, including empirical observations, expert interviews, primary, as well as secondary textual sources.[350]

Governmental Organizations' in Hendrik Hegemann, Regina Heller, and Martin Kahl (eds), *Studying 'Effectiveness' in International Relations: A Guide for Students and Scholars* (Verlag Barbara Budrich 2012). Moreover, goals are often subject to revisions, resulting from changes in policy contexts.

348 Elisabeth Corell and Michele M Betsill, 'Analytical Framework: Assessing the Influence of NGO Diplomats' in *NGO Diplomacy* (2007, The MIT Press 2007) ⟨https://perma.cc/6EV3-4YP6⟩; Dany (n 347).

349 Corell and Betsill (n 348) 32.

350 Betsill and Corell (n 328). Using different data types and sources helps increase confidence in relevant findings and allows for more solid case insights.

For purposes of illustration, if the evidence retrieved, empirical (e.g. statements made by interview partners) or theoretical (e.g. secondary academic literature), suggests that non-state actor (x) has issued concrete norms proposals and has supplemented these proposals with concrete measures, e.g. organisational adjustments, dedicated advocacy measures or the like, then non-state actor (x) has demonstrated high output effectiveness. In addition, if the evidence retrieved indicates that non-state actor (x) has succeeded at changing ego (e.g. realignment of operational strategies) and alter behaviours and has obtained commitments from other (relevant) actors, then non-state actor (x) has demonstrated high levels of outcome effectiveness. Furthermore, if the data acquired suggest that non-state actor (x) has achieved stated (policy) goals and has markedly reduced levels of cyberinsecurity, then non-state actor (x) has succeeded at effectuating systemic changes. These evaluation logics can also result in medium or low scores, depending on the degrees of influence yielded (please refer to the corresponding benchmarks recorded in Table 3.3).

	Output	**Outcome**	**Impact**
High	Issuance of concrete proposals which are embedded in operational strategies; dedicated policy work surrounding proposals issued.	Changes in ego and alter behaviours; policy commitments of targeted groups; wider referencing of initiatives across other fora.	Achievement of stated goals; reduction in numbers of cybersecurity incidents; increase in perceived levels of cybersecurity.
Medium	Publication of normative commitments but spotty operational follow-through, and strategic embeddedness.	Rudimentary changes in behaviour among agents; lip service and pro forma changes in organisational structures.	Implementation of quick-wins and short-lived cybersecurity initiatives.
Low	No clear/low commitments to normative ideas.	No/low changes in ego and alter behaviours; no/low changes in organisational structures.	No/low changes in levels of cybersecurity; proliferation of cybersecurity incidents.

Table 3.3: Effectiveness Indicators.

For all actors surveyed, the degrees of influence yielded across the dimensions of output, outcome, and impact will be summarised in tabular and visual forms (see Figure 3.3).

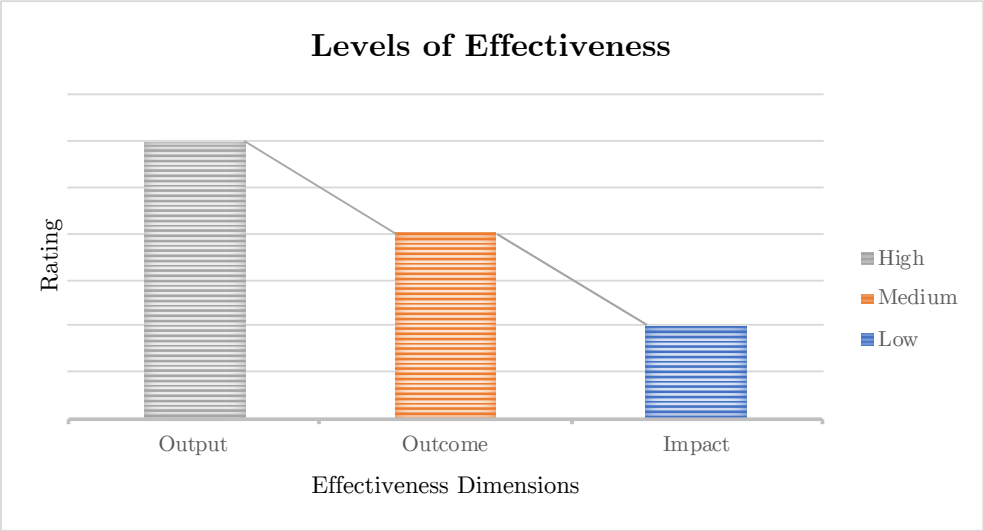

Figure 3.3: Example of Effectiveness Plot.

3.4 Limitations and Summary

Despite increasing levels of popularity across disciplines such as international relations and international law, qualitative research methods generally, and case study-oriented research approaches particularly have often been criticised for being 'biased, small scale, anecdotal, and/or lacking rigour'.[351] Among other things, critics have argued that 'the use of case [studies] absolves the author from any kind of methodological considerations. Case studies have become in many cases a synonym for free-form research where everything goes . . . '.[352] In addition, critics have called into question

[351] Claire Anderson, 'Presenting and Evaluating Qualitative Research' (2010) 74(8) American Journal of Pharmaceutical Education 141 ⟨https://perma.cc/ADF7-HM28⟩, 2.

[352] Zeev Maoz, 'Case Study Methodology in International Studies: From Storytelling to Hypothesis Testing' in Michael Brecher and Frank P Harvey (eds), *Millennial Reflections on International Studies* (University of Michigan Press 2002) 458.

standards of external validity or generalisability, and (researcher) objectivity. Cognisant of these criticisms, this thesis has endeavoured to limit potential methodological pitfalls to the greatest extent possible, i.e. by consciously triangulating different data points and applying consistent frameworks across the case studies under investigation.[353]

Regardless of these efforts, however, it is worth bearing in mind the following limitations relating to aspects of sampling and data availability, as well as investigative scope when engaging with this monograph. With regard to sampling and data availability it has to be noted that the universe of potential cases showcasing different roles taken on by non-state actors in cybersecurity norm creation project is not limited to the nine examples chosen for analysis. Indeed, the universe of cases is much larger. To ensure manageability of the project, however, pragmatic choices concerning the selection of empirical examples had to be taken. One key factor informing the selection of case studies was data availability. Even though cybersecurity- and norms-related inquiries have become more prevalent, data concerning the contributions of non-state actors to cybersecurity governance projects have remained relatively scarce, sometimes shrouded in secrecy, especially in instances when non-state actors cooperate with public actors, or when overshadowed by commercial or public policy interests. The results of this thesis have to be understood within these empirical limitations.

Apropos investigative scope, readers of this thesis are well advised to keep in mind that the range of materials suit for examination was limited to artefacts available in English, German, and French, three languages the author has reading proficiency in. The author abstained from using free online translation services, e.g. Google Translate, for documents published in other languages for reasons of potential misrepresentation

[353] For instance, with a view to preventing misleading interpretations and over-representation of the views gathered as part of the expert consultations, relevant data were triangulated with insights obtained from process observations and document reviews.

and loss of nuance. To ensure high levels of replicability and traceability all relevant online artefacts informing the findings of this thesis were archived using perma.cc.[354]

To recapitulate, this chapter has introduced readers to the main philosophical, ontological, epistemological and methodological considerations underpinning this manuscript. It has acquainted them with the cases selected for analysis, presented the main data collection and analysis strategies, and has commented on the limitations pertaining to the examination at hand. In seeking to respond to the research question introduced earlier, this chapter has argued that by using different qualitative data collection methods, more granular understandings of the roles taken on by non-state actors in cybersecurity norm formation projects can be obtained. In terms of methodological considerations, strategies of both depth and breadth were pursued.

The next chapters, i.e. *Chapters 4*, *5*, and *6*, review and examine in depth leading private endeavours pertaining to the construction of cybersecurity norms across the three stakeholder clusters introduced earlier, i.e. (a) civil society and academia, (b) corporate actors, and (c) expert communities. *Chapter 4*, Civil Society and Academia, will analyse and assess the activities of the following entities: (a) Global Partners Digital, (b) the second International Group of Experts, as well as (c) the Hague Program for Cyber Norms, while *Chapters 5* and *6* will look at endeavours pursued by (d) Microsoft, (e) Siemens, and (f) Kaspersky Lab, and (g) the Global Commission on the Stability of Cyberspace, (h) the Forum of Incident Response and Security Teams, and (i) Carnegie Endowment for Peace, respectively. Analysing the norms-related activities conducted by these actors will help better grasp the potentials as well as boundaries of private regulatory undertakings vis-à-vis increasing global cyberstability.[355] The case study chapters will show that non-state actors have developed

[354] See About (n 304).

[355] Flohr and others, *The Role of Business in Global Governance* (n 219).

distinctive approaches to debates about rules of the road for cyberspace. The spectrum of initiatives has come to include

> norm development and promotion with regard to state and industry behaviours; awareness-raising on threats and protection methods among technology developer and end-user communities; capacity building in the private sector and among the general public through education and engagement in public-private partnerships; information exchange[s] and the sharing of best practice[s]; the development of industry/sectoral norms through standardisation e.g. in software assurance and secure development practices and in agreeing standards for *privacy by default and security by design*; and initiatives in transparency and vulnerability/breach notification.[356]

[356] Paul Cornish and Camino Kavanagh, *Geneva Dialogue on Responsible Behaviour Phase One Report* (techspace rep, 2019) ⟨https://perma.cc/7P95-Z2DZ⟩ 15.

... [T]he very nature of cyberspace, the broad range of normative concerns involved, and the range of behaviours that pose risks to the maintenance of international peace and security call for much deeper – and possibly more responsible – civil society engagement than experienced in other areas. Such engagement can afford greater legitimacy and sustainability to ongoing multilateral processes concerning international security and ICT. It can also help ensure that normative concerns are attended to, and that the right technical expertise is leveraged when solutions are sought.

— Camino Kavanagh and Paul Cornish, *Geneva Dialogue on Responsible Behaviour in Cyberspace Phase One Report (2019)*

4

Civil Society and Academia

Contents

This chapter analyses the contents and evaluates the effectiveness of the normative efforts undertaken by civil society and academic organisations in the remit of developing rules of the road for the digital realm. Specifically, this chapter studies the activities undertaken by (a) *Global Partners Digital*, (b) the second *International Group of Experts*, and (c) the *Hague Program for Cyber Norms*. Structurally, the case studies proceed along three main parts. First, actor- and context-relevant details are provided. Second, key activities and roles executed by the relevant actors are analysed, and third, levels of effectiveness relating to the activities carried out by the latter are evaluated.

The chapter shows that in the remit of developing rules of the road for cyberspace, civil society and academic actors have made sensitising, structural, substantive, as well

as procedural contributions, and have chiefly acted as knowledge brokers and discussion feeders, as well as awareness raisers. In addition, they have inspired legal positioning and cross-sectoral collaboration. In terms of effectiveness, all of the actors studied as part of this chapter have displayed high scores across the output dimension, while showing varying results across the outcome and impact dimensions.

For the purposes of this study, civil society organisations (CSOs) are understood to comprise a 'wide array of non-governmental and not for profit organisations that have a presence in public life, express the interests and values of their members and others, based on ethical, cultural, political, scientific, religious or philanthropic considerations'.[357] Often referred to as third sector organisations (as opposed to the public and private sectors), they encompass a broad spectrum of entities such as academic institutes, trade and labour unions, human rights advocacy groups, faith-based entities and religious leaders, online networks and communities, consumer protection bodies, charitable organisations and foundations, environmental and peace activists, relief organisations, social movements, ethnic lobbies, as well as women and youth campaigns, among others.[358] To account for the diversity of entities, this thesis considers organisations or activities to belong to civil society 'when they involve a deliberate attempt – from outside the state and the market, and in one or the other organised fashion – to shape policies, norms and/or deeper social structures'.[359]

Organisationally, CSOs include both formal groupings as well as informal associations and entities. According to Schwab, 'civil society today includes an ever wider and more vibrant range of organised and unorganised groups, as new civil society

---

[357] World Bank, Civil Society (2020) ⟨https://perma.cc/ZU4Q-97YJ⟩ accessed 29 August 2020.

[358] Jan Aart Scholte, 'Global Civil Society: Changing the World?' (Warwick, 1999) ⟨https://perma.cc/QJ2G-R7V5⟩; Raffaele Marchetti, Global Civil Society (2016) ⟨https://perma.cc/69H6-WEB8⟩ accessed 6 May 2020.

[359] Scholte, 'Global Civil Society: Changing the World?' (n 358) 4.

actors blur the boundaries between sectors and experiment with new organisational forms, both online and off'.[360]

Since the 1990s, questions related to transnational civil society organisations have attracted considerable academic interest and spawned large numbers of research products.[361] Eminent works issued by authors including Margaret Keck, Kathryn Sikkink, Martha Finnemore, Thomas Risse-Kappen, and Ann Florini, for instance, have demonstrated that civil society actors have come to execute important tasks in endeavours pertaining to the (re)solution of complex global policy and security issues, including climate change, human rights, as well as land mines, and nuclear weapons.[362] Among other things, CSOs have been seen to shape policy agendas and raise awareness, increase policy responsiveness and transparency, deliver services, implement disaster management, preparedness and emergency strategies, conduct reviews and monitor the enforcement of reform activities, etc.

At times, governments have displayed ambivalent reactions towards the presence of and activities undertaken by CSOs in global politics. With regard to cybersecurity norm development, however, states have been fairly forthright about their inability to solve ICT-related challenges by themselves, and have called on non-governmental actors, including corporate as well as civil society entities for support. For example, in the 2010 UN GGE report, member states held that

> [c]onfronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international

---

360 World Economic Forum, *The Future Role of Civil Society* (techspace rep, January, World Economic Forum 2013) ⟨https://perma.cc/8DJX-SNDV⟩.

361 Ruggie, 'Reconstituting the Global Public Domain - Issues, Actors, and Practices' (n 51).

362 Keck and Sikkink (n 229); Risse-Kappen, Ropp, and Sikkink (n 178); Ann Florini, *The Third Force: The Rise of Transnational Civil Society* (Ebook central, Japan Center for International Exchange 2000); Kavanagh and Stauffacher (n 13).

> cooperation to be effective. Therefore, the international community should examine the need for cooperative actions and mechanisms ... .[363]

As part of the 2015 UN GGE consensus document, they maintained that

> [w]hile States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organisations ... [(particularly as they relate to ICT security capacity building]).[364]

Despite these appeals, and even though CSOs as well as other non-governmental stakeholders constitute critical elements in global ICT value chains and hold opinions apropos how to go about addressing security issues raised by digital technologies, research and academic commentary on their contributions to cybersecurity norm development processes have been limited.[365] This chapter seeks to address these pitfalls, and shed light on the roles taken on by these actors vis-à-vis increasing the security and stability of cyberspace. As per Kavanagh and Stauffacher,

> the expertise, knowledge and reach of these groups is fundamental to resolving or responding to many of the core technical problems inherent in the ICT environment and many of the insecurities and mistrust that has emerged between and within states regarding the uses of ICTs.[366]

Hence, more thorough examinations relating to these actors as well as their activities are critical.

The next sections survey the normative endeavours conducted by the three representatives of the civil society and academia cluster, namely (a) Global Partners Digital, (b)

---

[363] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 23) para. 15.

[364] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26) para. 31.

[365] Kavanagh and Stauffacher (n 13).

[366] Ibid 9.

the second International Group of Experts, as well as (c) the Hague Program for Cyber Norms, and evaluate the effectiveness of their activities with help of the frameworks developed as part of *Chapter 3*. Global Partners Digital, a human rights-oriented civil society organisation, will be the first case under investigation.

4.1 Global Partners Digital: Feeding Ideological Flames

A small-sized, London-based social purpose company, comprising 14 members of staff and endowed with net assets of GBP 307,133, Global Partners Digital has been active in the areas of cybersecurity policy and digital human rights since 2013.[367] Supported by a Board of Advisers composed of exclusively Western policy experts, Global Partners Digital seeks to instil democratic values and human rights in discussions relating to global ICTs.[368]

4.1.1 Background: Directing Attention to Human Rights

In terms of book of work, Global Partners Digital operates across three main issue areas: (a) emerging technologies, (b) trust and security, and (c) online content.[369] As a CSO, it relies on financial contributions from a broad range of funders to carry out its activities across the aforementioned areas, including public actors, corporate entities, as well as foundations. A careful reading of the list of sponsors, both past and present, reveals that

[367] Before 2013, Global Partners Digital operated as Global Partners and Associates (GPA). With the unprecedented growth of digital systems and infrastructures and related challenges and opportunities, GPA shifted its focus from traditional media, governance, and human rights issues to digital concerns, and re-branded accordingly, see Devex, Global Partners Digital (2020) ⟨https://perma.cc/267W-R539⟩ accessed 29 August 2020.

[368] Global Partners Digital, Who We Are (2020) ⟨https://perma.cc/Q2TC-LLJC⟩ accessed 29 August 2020. For an overview of the board members, please refer to Global Partners Digital, Board of Advisors (2020) ⟨https://perma.cc/6DLL-XQAW⟩ accessed 21 September 2020.

[369] Global Partners Digital, Explore the Issues (2020) ⟨https://perma.cc/XN6S-XJK9⟩ accessed 21 September 2020.

the roster of supporters is heavily skewed towards entities headquartered in the US and in Europe. To date, Global Partners Digital has received contributions from the Australian Ministry of Foreign Affairs, the Dutch Ministry of Foreign Affairs, the European Commission, Facebook, the Finnish Ministry of Foreign Affairs, Ford Foundation, the Argentinian Ministry of Foreign Affairs, Google, the Great Britain China Centre, the Institute for War and Peace Reporting, Mozilla, the Norwegian Ministry of Foreign Affairs, the Open Technology Fund, the Swedish International Development Cooperation Agency, the UK Foreign and Commonwealth Office, UNESCO, as well as the US Department of State – Bureau of Democracy, Human Rights and Labour.[370] As per information published on Global Partners Digital's website, in accepting funding the organisation is guided by values including independence, transparency, and integrity.[371]

4.1.2 Mandate and Goals: Creating Conditions for Change

Global Partners Digital has committed itself to facilitating strategic, informed and coordinated engagement in ICT-related decision-making processes, and to making these processes more open, transparent and inclusive.[372] With a view to delivering on this mandate, Global Partners Digital has identified four key areas for action, including (a) conducting strategic advocacy, (b) building capacity and sustainability, (c) making issues accessible, and (d) forging collaboration.[373]

Re conducting strategic advocacy, Global Partners Digital has sought to develop and distribute 'resources and tools to make advocacy in [the digital policy space] more effective, impactful and strategic'.[374] To this end, Global Partners Digital has, for

370 Global Partners Digital, Financials and Reporting (2020) ⟨https://perma.cc/3S9C-8RWN⟩ accessed 29 August 2020.

371 Ibid.

372 Who We Are (n 368).

373 Global Partners Digital, Our Work (2020) ⟨https://perma.cc/239Q-R7QU⟩ accessed 29 August 2020.

374 Ibid.

instance, issued a *Framework for Multistakeholder Cyber Policy Development*.[375] The latter refers to a 13-page document, authored by the CSO's Managing Directors in 2018, which is intended to provide 'anyone who wants to create a multistakeholder[-based] cyberpolicy process, or assess and evaluate an existing one' with a workable tool-set.[376]

Apropos building capacity and increasing sustainability, Global Partners Digital has helped fellow public interest groups, particularly from the Global South, strengthen their interactions with decision makers through financial and organisational assistance as well as dedicated training efforts. Among other things, Global Partners Digital has launched a cybersecurity capacity building programme, funded by the Dutch Ministry of Foreign Affairs.[377] In response to growing levels of politicisation pertaining to digital technologies, Global Partners Digital has endeavoured to broaden civil society participation, and enable access to key policy issues, primarily through 'creating travel guides[,] demystifying key internet policy issues, supporting innovative mapping projects ..., [as well as] delivering public webinars, scoping reports, research, events, and targeted in-person trainings'.[378]

Over the years, Global Partners Digital has built a broad network of partners (both public and private), which have contributed to the execution of the CSO's mission and the provision of technical, political, and advocacy know-how. Pursuing inclusive engagement approaches, the civil society organisation has created 'spaces for joint initiatives and constructive dialogue among and across stakeholder groups' in fora such

---

375 Global Partners Digital, *Framework for Multistakeholder Cyber Policy Development* (techspace rep, Global Partners Digital 2018) ⟨https://perma.cc/88AN-8VNV⟩.

376 ibid 5. The Framework for Multistakeholder Cyber Policy Development unites four characteristics of multistakeholder-based processes (open and accessible; inclusive; consensus-driven; and transparent and accountable) with three policy development stages (formation, drafting, agreement) into a two-tiered matrix. Depending on the intended use, it can either be employed as a to-do list for creating multistakeholder-oriented cyberpolicy processes, or as a check list for evaluating cyberpolicy processes vis-à-vis the four multistakeholder characteristics.

377 Global Partners Digital, GPD Launches New Global Programme to Foster Inclusive Cyber Policy-Making Processes (2016) ⟨https://perma.cc/6CKL-RC7A⟩ accessed 29 August 2020.

378 Our Work (n 373).

as the ITU or the London Process.[379] In terms of establishing its web of contributors, Global Partners Digital has benefited from acting as the Secretariat of the Freedom Online Coalition, an alliance of 31 governments, working to advance internet freedom.[380]

4.1.3 Activities: Producing Accessible Insights

Since 2017, Global Partners Digital has become noticeably active in discussions concerning norms of responsible behaviour in cyberspace.[381] Apart from providing regular explainers and technical briefings about key policy venues and points of discussion covered at these meetings, Global Partners Digital has facilitated or co-hosted events concerning the implementation of norms agreed as part of the 2013 and 2015 meetings of the UN GGEs.[382] For Instance, in the context of the 2019 iteration of the Internet Governance Forum, Global Partners Digital supported the execution of a workshop on the functions of the technical community vis-à-vis promoting cybersecurity norms.[383] The CSO also participated in the 2019 edition of the UN IGF Best Practice Forum on Cybersecurity, which examined leading norms initiatives, such as the Paris Call, or the GCSC's Norm Package Singapore, and collected best practices around the implementation of the standards suggested as part of these proposals.[384] Together with

---

379 Global Forum on Cyber Expertise, Global Partners Digital (2020) ⟨https://perma.cc/8E5Z-BN9Q⟩ accessed 29 August 2020.

380 Freedom Online Coalition, Aims and Priorities (2020) ⟨https://perma.cc/D3BA-53K6⟩ accessed 29 August 2020.

381 Global Partners Digital, Trust and Security (2020) ⟨https://perma.cc/4DH5-2PC5⟩ accessed 29 August 2020.

382 For a collection of the research outputs issued by Global Partners Digital concerning norms of responsible behaviour in cyberspace, please consult the following web page: Global Partners Digital, Norms Search Results (2020) ⟨https://perma.cc/9QDS-UCJM⟩ accessed 29 August 2020.

383 United Kingdom's Multi-Stakeholder Advisory Group on Cyber Issues, *Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015* (techspace rep, Chatham House 2019) ⟨https://perma.cc/357C-4C7G⟩.

384 United Nations Internet Governance Forum, Best Practice Forum on Cybersecurity (2019) ⟨https://perma.cc/W5M4-NNP3⟩ accessed 7 December 2019.

13 fellow civil society organisations, Global Partners Digital also filed a submission to the UN General Assembly First Committee on Disarmament and International Security relating to cyberpeace and human security, which called for the implementation of already-agreed upon standards of appropriate behaviour in cyberspace, and better access for civil society organisations to UN OEWG and GGE processes.[385]

In seeking to raise awareness around issues concerning cybersecurity norms and their interaction with human rights, the CSO also joined forces with other non-state actors with a view to extending the volume of their voices as well as the reach of their efforts. For instance, in December 2019, Global Partners Digital provided input to the UN OEWG 'to inform the discussions and shape the outcomes of the Open-ended Working Group's report' re four areas, i.e. (a) existing and emerging threats in cyberspace; (b) norms, rules and principles; (c) capacity building; and (d) confidence building measures.[386] In February 2020, it endorsed a statement made by the Association for Progressive Communications (APC) at the second substantive session of the Open-ended Working Group on International Cybersecurity, which demanded a 'rights-based and inclusive approach to understanding threats in cyberspace, and acknowledgement of the importance of all relevant stakeholders for both implementation and development of measures to address cyberthreats'.[387] Global Partners Digital further underscored the need for human-centric and rights-based approaches to cybersecurity in its feedback on the Open-ended Working Group's initial pre-draft report on ICTs. In its submission, dated March 2020, it recommended the report further accentuate the roles of different actors in tackling cyberthreats, as well as in contributing to capacity

---

385 Association for Progressive Communications, Civil Society Statement to the UN General Assembly First Committee on Disarmament and International Security on Cyber Peace and Human Security (2019) ⟨https://perma.cc/2A8F-CDSC⟩ accessed 29 August 2020.

386 Global Partners Digital, *Our Input to the OEWG Intersessional* (techspace rep, 2019) ⟨https://perma.cc/74KR-Q3KT⟩.

387 Association for Progressive Communications, APC Statement at the UN Open-ended Working Group on International Cybersecurity (2020) ⟨https://perma.cc/46MY-8X8E⟩ accessed 29 August 2020.

and confidence-building measures. The CSO also suggested the report acknowledge the roles of non-governmental stakeholders in supporting the implementation of the eleven norms stipulated by the UN GGE in 2015, i.e. including through 'raising awareness and socialising the norms, capacity building, monitoring implementation, providing evidence-based research, and proposing specific technical and policy solutions [concerning the implementation of] the norms'.[388]

Consistent with its overarching mandate, Global Partners Digital also advocated for the creation of 'inclusive, consensus-driven, sustainable, and results-oriented' platforms for regular institutional dialogue.[389]

4.1.4 Role Profiles: Advocating Strategically and Building Awareness

With regard to its cybersecurity norms-oriented activities, Global Partners Digital has primarily acted as advocacy-oriented awareness raiser. Awareness raisers seek to disseminate ideas and pertinent information concerning relevant policy issues among distinctive networks or wider audiences with the aim of informing and changing their perceptions, behaviours, and beliefs towards the achievement of specified social/political objectives and goals.[390] As entities dedicated to effecting wide-ranging policy transformations, CSOs have been seen to resort to awareness-raising strategies rather frequently. In terms of theoretical underpinnings, public awareness-raising and advocacy efforts have borrowed from concepts of mass communication and social change marketing. The latter involve the application of different marketing techniques and tools to salient

388 Global Partners Digital, *Pre-Draft of the OEWG's Report on ICTs* (techspace rep, 2020) ⟨https://perma.cc/T9RU-BHAM⟩.

389 Ibid.

390 Richard Sayers, *Principles of Awareness-Raising: Information Literacy, a Case Study* (techspace rep, UNESCO 2006) ⟨https://perma.cc/L5XC-SKAV⟩.

policy issues with the intention of bringing about behavioural alterations.[391]

In addition to communicative practices, awareness-raising efforts often include educational and constructive elements. Awareness-raising activities go hand in hand with increasing issue-related levels of visibility and credibility among members of specific communities.[392] As per Sayers, common approaches and techniques for raising public awareness include, among others, engaging in (personal) exchanges with target audiences by means of holding or participating in public meetings, conferences, specialist workshops and informal social events; leading training programmes across international policy venues; issuing educational and research materials, including, for example, reports, digests, briefings, commentaries, or written submissions; hosting and maintaining online presences, email discussion lists and blog entries; engaging with media outlets, giving interviews or publishing articles in newspapers, magazines or electronic resources; forming strategic partnerships and alliances with like-minded organisations, including fellow civil society organisations; as well as conducting political lobbying activities.[393]

Global Partners Digital has used several of these tools to raise awareness for cybersecurity norms-related issues. For instance, in line with the different activities outlined in the previous section, Global Partners Digital has issued briefings on inclusive stakeholder engagement strategies, and emphasised 'the need for transparency and openness in order to ensure meaningful input' from non-state entities to cybersecurity norm development processes in the context of the 2019 UN General Assembly First Committee Group of Governmental Experts (GGE) and Open-ended Working Group (OEWG) meetings.[394] In addition to drafting briefings directed at member states,

391 Sayers (n 390). In contrast to awareness-raising practices, advocacy activities are more targeted in terms of addressees, often directed at decision makers, see Bernard Enjolras and Karl Henrik Sivesind, *Civil Society in Comparative Perspective* (Emerald Group Publishing 2009) 183.

392 Ibid.

393 Sayers (n 390).

394 Global Partners Digital, Measures for Stakeholder Engagement in the UN Group of Governmental Experts and Open-Ended Working Group A Global Partners Digital Briefing (2019) ⟨https://perma.cc/6AHQ-FRZ8⟩ accessed 29 August 2020.

Global Partners Digital has also actively participated in corresponding meetings, e.g. the first organisational meeting of the OEWG, or the UNIDIR Cyber Stability Conference, where the CSO reiterated the importance of stakeholder diversity in the context of cybersecurity norm development processes.[395] Along with awareness-raising activities revolving around procedural aspects, i.e. broader stakeholder engagement, Global Partners Digital has also submitted sensitising pledges pertaining to rules of the road for cyberspace, in particular with regard to how discussions about peace and security in the virtual realm relate to and affect the protection of human rights.[396] For instance, in its submission to the informal intersessional consultative meeting of the OEWG with industry, non-governmental organisations and academia, Global Partners Digital put forward that

> ... [e]ach of the [eleven] norms listed in paragraph 1 of General Assembly resolution 73/271 has a link with human rights. In particular, the implementation of each norm can result in a negative or beneficial impact on human rights. Civil society has an important role to play in shaping and implementing the norms and thereby in supporting state actors in their responsibility to promote a secure and stable cyberspace. ... The OEWG should recognise the important role of all stakeholders, including civil society, in implementing the [eleven] norms. During forthcoming meetings of the OEWG, states should be encouraged to share their experiences and challenges in implementing the norms. Furthermore, it should recognise the importance of accountability in ensuring operationalisation of the norms. Therefore, going forward, the OEWG should recommend instituting a reporting process that provides periodic and publicly available assessments of states adherence to the norms.[397]

According to Expert #14, Global Partners Digital has engaged in diplomatic awareness-raising efforts at various levels, including at semi-formal (track 1.5 diplomacy) and informal (track 2.0 diplomacy) levels.[398] As per Expert #23, CSOs which have

---

[395] Global Partners Digital, Cyber Norms in NYC: Takeaways From the OEWG Meeting and UNIDIR Cyber Stability Conference (2019) ⟨https://perma.cc/T5G7-V3SK⟩ accessed 29 August 2020.

[396] Global Partners Digital, *Our Input to the OEWG Intersessional* (n 386).

[397] Ibid 2.

[398] Expert #14, Interview #14 (2019).

traditionally been concerned with protecting human rights online have been seen to contribute to cybersecurity norms-related discussion fairly actively. In terms of the nature of their contributions, Expert #23 emphasised their awareness-building roles:

> I see them engaging through advocacy. I see them, raise awareness, I see them at a lot of the meetings within either the United Nations ..., or even within our own events. They are present, they voice their perspectives, their suggestions, their concerns. ... And then of course, you see them online, through policy papers, through memos, through op-eds, through reports. These are the platforms and the mediums that come to mind.[399]

The diversity of tools employed by Global Partners Digital as well as the partnerships initiated with organisations such as the Association for Progressive Communication, Derechos Digitales, or Access Now, have helped its cybersecurity norms-related messages be transported to and received by broad audiences. Successful awareness-raising campaigns usually home in on one key message or 'a suite of closely related subsidiary messages'.[400] In the case of Global Partners Digital, their awareness-raising activities have revolved around two main issues, (a) ensuring broad stakeholder engagement, procedurally but also in terms of content, and (b) promoting human (rights)-centric approaches in discussions about rules of the road for cyberspace. The timing of their awareness-raising activities has been closely aligned with international cybersecurity policy meetings and directed at both, representatives of member states taking part in debates about norms of responsible behaviour in cyberspace, and broader audiences following these discussions.

An empirically less discernible role played by Global Partners Digital is the role of implementation assistant and capacity builder. Implementation assistants actively work towards or meaningfully support the execution and delivery of policy prescriptions.

---

399 Expert #23, Interview #23 (2019).

400 Sayers (n 390) 16.

Where implementation assistants do not engage in direct actions, they 'offer technical advice and expertise' concerning the delivery of relevant prescriptions.[401]

According to Pollard and Court, CSOs

> contributing to implementation through technical assistance must be as adept in using their knowledge in an appropriate way. To ensure that technical understanding does not dominate the knowledge of others, they must foster a *learning approach*, and be able to translate their expertise into tacit and implicit as well as explicit forms.[402]

Global Partners Digital has issued implementation recommendations. With regard to the 2015 UN GGE norms, for instance, Global Partners Digital has actively showcased areas for CSO-based implementation assistance. As per its brief referenced earlier, CSOs have important parts to play in delivering the eleven normative stipulations contained in the 2015 UN GGE consensus report, ranging from documenting and calling out state-led network disruptions, surveillance efforts, or censorship activities, to supporting attribution endeavours, and conducting simulation exercises and training sessions pertaining to the protection of critical infrastructures, or monitoring compliance with human rights standards across ICT supply chains.[403] In highlighting areas for CSO-contributions and calling to action fellow non-state entities, Global Partners Digital has supplied concrete, implementation-oriented guidance. The social purpose company has also given new weight to calls for more extensive civil society engagement, and has strengthened voices who have claimed that 'such engagement ... can afford greater legitimacy and sustainability to on-going multilateral norms and CBM processes concerning international security and state uses of ICTs'.[404] Greater civil society participation can also help 'ensure that broader normative concerns are attended to,

---

401 Amy Pollard and Julius Court, 'How Civil Society Organisations Use Evidence to Influence Policy Processes: A Literature Review' (London, 2005) ⟨https://perma.cc/7K3V-9KBG⟩ 18.

402 Ibid 19.

403 Global Partners Digital, *Our Input to the OEWG Intersessional* (n 386) 2.

404 Kavanagh and Stauffacher (n 13) 2.

and that the right technical expertise is leveraged when solutions are being sought', which in turn can aid the creation of more trusted relationships among state and non-state actors.[405]

4.1.5 Effectiveness Review: Fighting to Effect Behavioural Alterations

In concurrence with the conceptual remarks presented in *Chapter 3*, this section evaluates the effectiveness of the norms-related undertakings conducted by Global Partners Digital. As aptly argued by Flohr and others, '[i]n policy research, effectiveness is the most important yardstick for the evaluation of private [, i.e. non-state,] contributions to governance'.[406] In seeking to add to policy-relevant analyses, this thesis assesses the effectiveness of private ideational contributions along the dimensions of output, outcome, and impact, thereby taking into account both actor-level and structural elements, and assigns corresponding ratings of low, medium, or high to the relevant dimensions. Evaluations of effectiveness help answer questions such as, *to what extent have non-state actors contributed to the successful management of transboundary problems?* And if they have made tangible contributions, *by which means and through which activities?*[407]

Output

Between 2015 and 2020, Global Partners Digital has published more than 50 norms-related assets, comprising blog posts, explainers, digests, and policy submissions.[408] By so doing, the CSO has actively supported processes of sense-making. In addition

405 Kavanagh and Stauffacher (n 13) 2.

406 Flohr and others, *The Role of Business in Global Governance* (n 219) 169.

407 Ulbert (n 50).

408 Norms Search Results (n 382).

to issuing information-aggregating artefacts, the social purpose company has also introduced highly practical elements, including, for instance, a global calendar of major cyberevents. As per the CSO,

> there is a growing need for human rights defenders to engage in relevant policy processes [pertaining to cybersecurity]. However, the policy landscape is complex and difficult to navigate. [The] calendar seeks to address this by mapping the key events and processes which shape the global cybersecurity policy landscape, and highlighting those that matter most for human rights defenders.[409]

Rather than devising new normative proposals, Global Partners Digital has been adamant about highlighting the human rights-related dimensions in discussions about rules of the road for cyberspace, and has actively and consistently called for the integration of human rights concerns into cybersecurity norm construction processes. Indeed, the social purpose company has succeeded at submitting these concerns to international fora, and onto the radar screens of policymakers preoccupied with promoting rules of the road for cyberspace. In terms of normative commitments, Global Partners Digital has abstained from endorsing specific initiatives such as the Paris Call for Trust and Security in Cyberspace launched by the French Ministry of Foreign Affairs in collaboration with Microsoft, or the Norm Package Singapore issued by the Global Commission on the Stability of Cyberspace. Instead, it has consciously sought to create and leverage links between its mission, i.e. to '[bring] laws and policies relating to the digital environment more in line with international human rights standards' and international discussions about cybersecurity norms.[410]

As is evident from the remarks above, normative concerns have become deeply embedded into the organisation's strategies and activities. Global Partners Digital has dedicated significant financial as well as human resources to advancing the organisation's

---

[409] Global Partners Digital, Cyber Events Calendar (2020) ⟨https://perma.cc/AHS8-947C⟩ accessed 1 September 2020.

[410] Who We Are (n 368).

interests and viewpoints in these deliberations and has conducted considerable amounts of policy work around these debates. Hence, in line with the operationalisation of the different components outlined in *Chapter 3*, Global Partners Digital has been very effective across the dimension of output.

Outcome

In terms of outcome, the activities undertaken by Global Partners Digital in the context of promoting rules of the road for cyberspace have yielded little success. While the CSO has managed to find allies in and form coalitions with other non-state actors, e.g. Access Now, Derechos Digitales, or Association for Progressive Communications to promote human-centric and rights-based approaches, explicit references to and specifications of those concepts across international cybersecurity norm construction venues have been sparse, with the exception of one mention of the word human-centric in paragraph four of the Open-ended Working Group's *Second Pre-draft Report*.[411] Indeed, in the context of the CSO's submission to the Global Commission on the Stability of Cyberspace, none of its recommendations submitted have found mention in the Commission's final report.[412] While the promotion, protection, and enjoyment of human rights and fundamental freedoms have been referenced across the Paris Call for Trust and Security in Cyberspace, the final report of the Global Commission on the Stability of Cyberspace, as well as the *Second Pre-draft of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security*, other proposals and bids for clarifications tendered

[411] Civil Society Statement to the UN General Assembly First Committee on Disarmament and International Security on Cyber Peace and Human Security (n 385).

[412] Global Partners Digital, *Our Submission to the Global Commission on the Stability of Cyberspace's Request for Consultation on the Norm Package Singapore* (techspace rep, Global Partners Digital 2019) ⟨https://perma.cc/Q5D4-K5Y5⟩.

by Global Partners Digital have not been referenced.[413] It is hard to argue that the broad references to human rights across these documents have been the results of the activities undertaken by Global Partners Digital.

Although having had little effects on the behaviours of third parties, the social purpose company has managed to be a present and constant voice in discussions about rules of the road for cyberspace and has actively used platforms, including the United Nations Internet Governance Forum, to broaden the scope of its audiences and create awareness for human rights concerns across various cybersecurity norm formation processes. Procedurally, the CSO has reaffirmed the importance of non-state actors being present at relevant norm formation venues and has actively helped build access to those venues for third parties by providing relevant information and building capacity.

Impact

From a systemic perspective, the activities undertaken by Global Partners Digital have had little effects on global levels of cybersecurity. According to Flohr and others, the impact dimension takes into account 'an institution's contributions to problem solving, which are considered effective if problems that led to the creation of an institution are solved or at least alleviated'.[414] Instead of greater promotion and protection, human rights online have experienced further curtailing and infringement in recent years, and the normative baselines underpinning these inalienable rights have become porous, and have encountered more disrespect than enforcement or support. Cybersecurity has often served as pretext to justify exceptions to human rights, weaken encryption standards and introduce back-doors into products used by members of society.[415] Civil

[413] United Nations Open-ended Working Group, *Second Pre-Draft of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, United Nations 2020) ⟨https://perma.cc/6ADQ-TF2D⟩; Global Partners Digital, *Pre-Draft of the OEWG's Report on ICTs* (n 388).

[414] Flohr and others, *The Role of Business in Global Governance* (n 219) 173.

[415] Geneva Internet Platform Digital Watch, A Rights-Based Approach to Cybersecurity (2017) ⟨https://perma.cc/DF63-9MH5⟩ accessed 4 September 2020.

society-organised discussions about rules of the road for the virtual realm have not stopped governments, including China and Russia, from conducting extensive spyware-based surveillance operations against members of civil society, and in particular human rights defenders and journalists.[416]

According to Freedom House, *Freedom on the Net* declined for the ninth year in a row in 2019.[417] As per the report, respect for human rights in the virtual realm is

> increasingly imperilled by the tools and tactics of digital authoritarianism, which have spread rapidly around the globe. Repressive regimes, elected incumbents with authoritarian ambitions, and unscrupulous partisan operatives have exploited the unregulated spaces of social media platforms, converting them into instruments for political distortion and societal control. ... Moreover, a startling variety of governments are deploying advanced tools to identify and monitor users on an immense scale.[418]

While the CSO's mission to 'enable a digital environment underpinned by human rights' has proven difficult to achieve, and broad system-level behavioural alterations do not appear to have materialised, Global Partners Digital has made contributions in terms of broadening the webs of civil society organisations contributing to problem solving efforts in the areas of cybersecurity norms and human rights.[419] Hence, procedurally Global Partners Digital has been successful at extending awareness-related ideational boundaries and easing access to debates about rules of the road for cyberspace.

4.1.6 Précis

This section has studied the cybersecurity norm promotion efforts conducted by Global Partners Digital, a small, human rights-oriented social purpose company based

---

416 Citizen Lab, NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases (2019) ⟨https://perma.cc/H9JG-98C5⟩ accessed 3 September 2020.

417 Freedom House, *Freedom on the Net 2019: The Crisis of Social Media* (techspace rep, Freedom House 2019) ⟨https://perma.cc/SE35-THYC⟩.

418 Ibid 1.

419 Who We Are (n 368).

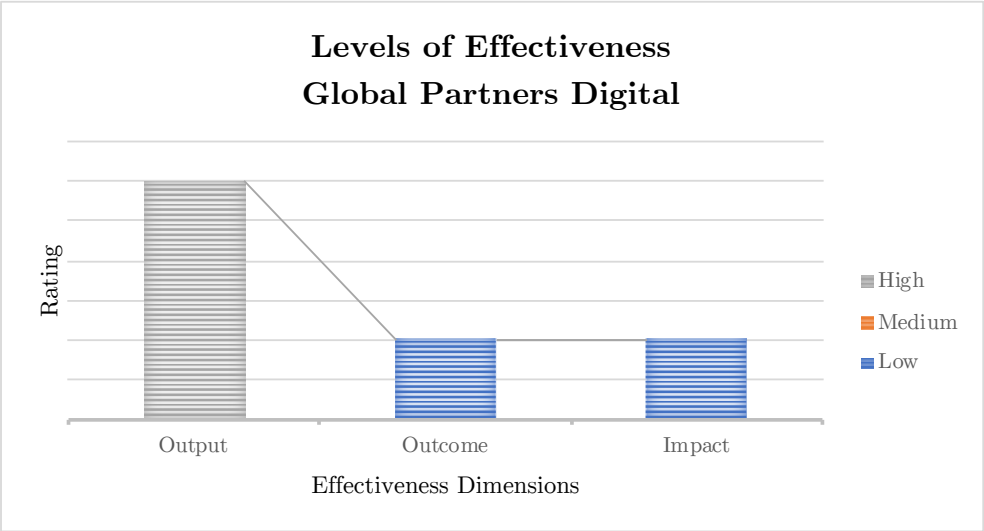

Figure 4.1: Effectiveness Plot: Global Partners Digital.

in London. Supported by funding from pro-cybersecurity norms bodies, including the Ministries of Foreign Affairs of the Netherlands and Australia, as well as the European Commission, Global Partners Digital has become a constant and present voice in international debates about rules of the road for cyberspace. In line with its mission, the CSO has primarily acted as awareness raiser for human rights-related concerns in discussions pertaining to responsible behaviour in the virtual realm but has also been seen to support ideational implementation efforts by means of offering technical advice and expertise.

In terms of output the CSO has generated remarkable numbers of information-condensing artefacts and has conducted considerable amounts of policy work around these debates. As regards outcome and impact, its efforts have been less effective. Although Global Partners Digital has managed to foster and enter into collaborative arrangements with other non-state actors, changes in behaviours of third parties and inclusion of the CSO's proposals into global policy documents pertaining to rules of the road for cyberspace have been sparse. In the context of promoting peace and security in

	Output	Outcome	Impact
High	Global Partners Digital has generated information-condensing artefacts and has conducted considerable amounts of policy work around these debates.	-	-
Medium	-	-	-
Low	-	The CSO has been a constant voice in discussions about rules of the road for cyberspace and has actively used multistakeholder platforms to create awareness for human rights concerns across various cybersecurity norm formation processes but has seen little uptake of the ideas proposed across these venues.	The activities undertaken by Global Partners Digital have had little effects on global levels of cybersecurity. Human rights online have experienced further curtailing and infringement in recent years.

Table 4.1: Effectiveness Review: Global Partners Digital.

the virtual realm, Global Partners Digital has, however served as a reminding voice to pay due regard to human rights-related concerns in debates about cybersecurity norms. It has also usefully extended access to these debates and has broadened boundaries of ideational awareness. The next section studies the norm-making activities carried out by the second International Group of Experts.

4.2 Second International Group of Experts: Inspiring Legal Positioning

Between 2009-2013 and 2013-2017, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), an interdisciplinary, NATO-accredited cyberdefence hub based in Tallinn, Estonia, invited two International Groups of Experts to examine

how extant international legal provisions, in particular jus ad bellum and jus in bello provisions, apply to cyberoperations. Primarily composed of decorated legal scholars as well as legal practitioners from institutions, including NATO's Allied Command Transformation, and the United States Cyber Command, the International Groups of Experts issued two consecutive Manuals, the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, an updated and expanded version of the first Manual. While the first edition of the Manual focused on identifying international rules applicable to cyberoperations above the threshold of use of force, i.e. in situations of armed conflict, the second version of the Manual pursued an extended mandate and also looked into pinpointing legal regimes implicated by peacetime cyberactivities, which do not meet the threshold of use of force according to Article 2(4) of the UN Charter.[420]

In asking two International Groups of Experts to study the applicability of international legal regimes and extant norms to complex new environments, NATO CCD COE followed earlier precedents,

> such as those resulting in the 1880 Oxford Manual, the International Institute of Humanitarian Law's 1994 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, and the Harvard Program on Humanitarian Policy and Conflict Research's 2009 Manual on International Law Applicable to Air and Missile Warfare.[421]

In line with the temporal focus of this manuscript, efforts pertaining to the second Tallinn Manual, i.e. norms-oriented activities conducted by the second International Group of Experts, are at the centre of analysis.

---

[420] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158).

[421] Ibid 1.

4.2.1 Background: Addressing Questions of International Law

Led by Michael N. Schmitt, Professor of Public International Law at Exeter Law School, Charles H. Stockton Professor at the United States Naval War College and Francis Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy at West Point, the second International Group of Experts consisted of 19 legal scholars and advisers. Table 9.2 listed in the *Appendix* provides an overview of the individuals appointed to the second International Group of Experts, their (previous/current) designations, as well as their institutional affiliations.

In response to concerns issued about limited geographic and substantive diversity vis-à-vis the first International Group of Experts – the first Group mainly included professionals from the Western hemisphere – composers of the second International Group of Experts endeavoured to ensure more diverse representation. Among others, the second International Group of Experts included representatives from Japan, China, and Kazakhstan, as well as specialists with substantive expertise in areas such as international human rights law, space law, and international telecommunications law.[422] While the record of experts (see Table 9.2 listed in the *Appendix*) undoubtedly conveys legal know-how and experience, Western mindsets appear to have retained their leading positions even as part of the second iteration, while experts from the Global South have been left out entirely, for instance. Even though, as argued by Heintschel von Heinegg, participants were primarily 'selected based on their mastery of the relevant law or their sensitivity to the cybercontexts in which that law would be applied, or both', the inclusion of expert voices from the Global South, would, at the very least, have increased the standing of the Group as well as the degrees of context specificity of the rules stipulated.[423]

---

[422] Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Inisghts' (2017) 43(3) Georgetown Journal of International Law 735 ⟨https://perma.cc/S22D-8JZE⟩.

[423] Wolff Heintschel von Heinegg, 'The Tallinn Manual and International Cyber Security Law' in *Yearbook of International Humanitarian Law 2012* (Springer 2012) 4.

With regard to the Group's authority, Director and General Editor, Professor Michael N. Schmitt, maintained that the second edition of the Manual

> is not an official document, but rather the product of two separate endeavours undertaken by groups of independent experts acting solely in their personal capacity [(emphasis added)]. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. Nor does it reflect the position of any other organisation or State represented by observers or of any of the States involved in the *Hague Process* ... . Finally, participation as members of the International Group of Experts or as peer reviewers by individuals who hold governmental positions in their respective countries must not be interpreted as indicating that the Manual echoes the viewpoints of those countries.[424]

With reference to Schmitt's remarks, the Tallinn Manual 2.0, just like its predecessor, should be regarded as an academic consensus document, which identifies existing rules applicable to cyberoperations as well as their relations to other specialised legal regimes, including human rights law, diplomatic law, space law and telecommunication law.[425]

4.2.2 Mandate and Goals: Providing Expert Guidance

In contrast to the first International Group of Experts, the second Group pursued a broader mandate. In addition to laying out the rules applicable to nefarious cyberactivities crossing the threshold of use of force (i.e. acts of cyberwar), the second Group also studied public international law norms governing cyberoperations during peacetime. Peacetime cyberoperations have seen much higher rates of prevalence than war-level cyberattacks.

As per the drafters' introductory remarks, the goal of the Tallinn Manual 2.0 was never to issue binding legal rules. Rather, the

> Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law. ... This

---

424 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158) 2.

425 Efrony and Shany (n 150).

> Manual is meant to be a reflection of the law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. It is not a *best practices* guide, does not represent *progressive development of the law*, and is policy and politics-neutral. In other words, Tallinn Manual 2.0 is intended as an objective restatement of the lex lata. Therefore, the Experts involved in both projects assiduously avoided including statements reflecting lex ferenda.[426]

The attempts undertaken by the two International Groups of Experts, i.e. identifying existing legal regimes and applying them to new contexts and environments, are 'part of a long-standing tradition of legal scholars and practitioners', seeking to extend existing laws through processes of interpretation and analogy rather than by devising new sets of rules.[427]

The rules issued by the drafters were primarily intended for governmental legal advisers responsible for providing senior public decision makers with (cybersecurity-related) international legal counsel. In a secondary instance the experts also hoped to inspire 'academic and other endeavours'.[428]

4.2.3 Activities: Interpreting Rules

The second International Group of Experts started its activities in 2013. Following four years of deliberations, it released 154 consensus-based rules applicable to cyberoperations as well as rich commentaries concerning the legal bases of each of those 154 rules and relevant grounds of interpretation, in February 2017.[429] The substance of the original Manual appeared in the second edition, 'though slightly altered to reflect points of clarification since [the Manual's] original publication'.[430]

---

426 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158) 2-3.

427 Efrony and Shany (n 150) 583.

428 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158) 2.

429 The first International Group of Experts issued 95 black letter rules.

430 Jensen (n 422) 737.

In addition to the legal experts listed in Table 9.2, the Manual benefited from inputs issued by experienced observers.[431] Initial drafts of rules and commentaries were put forward by subject matter experts (some of which were members of the second International Group of Experts), vetted by the Manual's editors, and then submitted to peer reviewers. Following the assessment of the peer reviewers, the rules and commentaries were then discussed/specified by the International Group of Experts in three one week-long sessions held between 2015 and 2016.[432] Subsequent to additional rounds of peer reviews and adjustments, the experts finalised their stipulations in April 2016. On top of the meetings of the second International Group of Experts, the Manual's sponsoring entity, NATO CCD COE, conducted several workshops on issues analysed as part of the Tallinn Manual 2.0, including, international human rights law and peacetime cyberespionage.[433]

In contrast to the first edition of the Manual, governments enjoyed greater exposure to the activities undertaken by the second International Group of Experts. As part of the *Hague Process* organised by the Dutch Ministry of Foreign Affairs, state representatives were able to comment on the draft rules and commentaries in an unofficial capacity. According to Schmitt, the three two-day sessions hosted by the Dutch Ministry of Foreign Affairs 'were attended by delegations from over 50 States and international organisations. ... [The Process] proved invaluable to the initiative, as the International Group of Experts was uniformly of the opinion that international law is made and authoritatively interpreted by States'.[434] While governmental representatives were able to issue comments, the drafters emphasised that the opinions expressed as part of the

[431] As per Schmitt, '[t]he observers participated fully in the discussions and drafting of the Manual, but their consent was not necessary to achieve the unanimity required for adoption of a rule', see Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158).

[432] Ibid.

[433] Ibid.

[434] Ibid 2.

Manual were exclusively the ones of the appointed experts, and did not represent specific state positions.

In terms of provisions stipulated, the majority of the 154 rules adopted relate to jus ad bellum and jus in bello issues (laws of war). In sum, the Tallinn Manual 2.0 consists of four parts. Part 1 covers questions pertaining to international law and cyberspace generally, including key principles such as sovereignty, due diligence, jurisdiction, and state responsibility. Cyberoperations not per se regulated by international law, e.g. peacetime espionage and non-state actors, also receive brief consideration. Part 2 examines the relations between cyberspace and specialised regimes of international law, including international human rights law, the law of the sea, diplomatic and consular law, as well as air, space, and international telecommunications law. Part 3 covers jus ad bellum provisions, and part 4 looks at jus in bello norms applicable to the virtual realm.[435]

The two Manuals have incited numerous reactions from public and private entities. The types of responses received relating to the Tallinn Manual 2.0 have ranged from encouraging messages of support to less enthusiastic expressions of criticism. Among other things, critics have found fault with the levels of clarity and granularity applied to jus ad bellum and jus in bello rules versus human rights rules, the latter having remained fairly high-level and vague.[436] As Ingber has fittingly stated,

> Tallinn 2.0 could not but inherit the granular in-the-weeds assessment of LOAC [(law of armed conflict)] rules as they apply in cyberspace, crafted in the Tallinn 1.0 process. In updating the Manual with a broader Group of Experts, Tallinn 2.0 may have updated the LOAC rules, but they and states had been living with the first Manual in existence at this point for four years, and the second Group of Experts would not have seen themselves as having a mandate or need to water them down for the purpose of levelling the playing field with other fields of law in Tallinn 2.0.[437]

---

435 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 158).

436 Rebecca Ingber, 'Interpretation Catalysts in Cyberspace' (2017) 95(7) Texas Law Review 1531 ⟨https://perma.cc/ZLC7-AFSY⟩.

437 Ibid 1550.

Commentators have also called into question the suggested impartiality of the International Group of Experts, given its extensive exchanges with governments, and criticised 'the ambiguity surrounding the authority of the Manual as reflective of international practice, as opposed to it being an articulation of the views of international experts on how international law should be applied to cyberoperations'.[438] Despite the valid points of criticism raised by observers, the Tallinn Manual 2.0 as well as its predecessor represent thorough and careful analyses of how different bodies of international law translate to cyberspace.[439]

4.2.4 Role Profiles: Moulding Customary Interactions

In concurrence with its mission, the second International Group of Experts has acted as active knowledge broker. It has made accessible and offered rich clarifications on how existing legal regimes relate to cyberoperations, and has demonstrated that cyberevents do not take place in legal vacuums. Knowledge brokers are specialists or association of specialists/organisations who seek to equip decision makers with relevant information and insights, and facilitate processes of learning and discussion. They forge and sustain connections between researchers and different audiences (government officials as well as practitioners) with shared concerns by means of making known and disseminating relevant research findings. 'Able to link know-how, know-why, and know-who', knowledge brokers work across public as well as private domains and boundaries, promote mutual understanding among target audiences, and help develop new capacities.[440] In the face of surging levels of convolution pertaining to global

[438] Efrony and Shany (n 150) 4.

[439] Eichensehr, 'Review of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)' (n 151).

[440] Morgan Meyer, 'The Rise of the Knowledge Broker' (2010) 32(1) Science Communication 118 ⟨https://perma.cc/2Z6Z-22R3⟩, 119.

policy matters, knowledge brokering has gained ground and has come to be viewed as a means to address 'wicked problems'.[441]

To effectively promulgate relevant insights, knowledge brokers 'engage in a set of relational, technical, and analytical activities that help communities of practice (CoPs) to develop and operate, ... and help groups and individuals to create, explore, and apply knowledge in their practice'.[442] Against the background of these qualities, knowledge brokers have also come to be referred to as *bridge builders*, linking knowledge producers with knowledge users.[443]

The knowledge-generating/building nature of the work conducted by the second International Group of Experts has been widely acknowledged by primary as well as secondary sources. Estonian President Kersti Kaljulaid, for instance, has argued that the

> Tallinn Manual 2.0 is by far one of the most comprehensive analyses of international law applicable to cyberoperations. For liberal democracies that respect the rule of law, international law undoubtedly shapes and bounds governments' activities. ... Cyber Operations have become an integral part of international relations – the recent launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations is a practical handbook for state legal advisers of how to deal with these issues. ... No other initiative in the world carries so comprehensive overview of many different experts from various countries.[444]

Commending the efforts of the International Group of Experts, Interviewee #9 has argued that

> [international law experts] cannot apply international law themselves, but they can propose [rules]. And I would say that they [(i.e. the members of

---

441 Justyna Bandola-Gill and Catherine Lyall, 'Knowledge Brokers and Policy Advice in Policy Formulation' in Michael Howlett and Ishani Mukherjee (eds), *Handbook of Policy Formulation* (Edward Elgar Publishing Ltd 2017).

442 James Conklin and others, 'Knowledge Brokers in a Knowledge Network: The Case of Seniors Health Research Transfer Network Knowledge Brokers' (2013) 8(1) Implementation Science 7 ⟨https://perma.cc/L3FH-CJNJ⟩, 1.

443 Ibid 1.

444 Kersti Kaljulaid, President of the Republic Opening Speech at CyCon 2017 (2017) ⟨https://perma.cc/QYJ3-45P4⟩ accessed 5 June 2020.

> the second International Group of Experts)] did a great job for governments. Now it is up to the legal advisers in the ministries and in the governments to look into what academia is proposing. I come from ... a small nation, our legal department was ten persons. We just did not have time to do all the academic work. So, we cooperated very closely with academia.[445]

Corroborating these perceptions, one of the legal peer reviewers of the Manual, Colonel Gary Corn, has held that the

> Tallinn Manual 2.0 makes a valuable contribution to the cornerstone premise that international law applies to cyberspace and to framing and advancing the knottier discussion of how it applies, even if States do not necessarily agree with every aspect of the Manual.[446]

Similarly, Barnsby and Reeves have declared that

> the Tallinn Manual 2.0 represents a tremendously useful starting point for assessing the challenging intersection of multiple areas of the law. ... [T]he above nuanced criticism is not a broad condemnation of the Group of Experts' efforts in any regard. To the contrary, it is only because of their excellent and unprecedented work that we are able to spot the definitional gaps and begin to fill them with evidence of State practice. All of it, and especially the IHRL [(International Human Rights Law)] chapter, represents a tremendous contribution to the law.[447]

Related to its knowledge brokering function, the second International Group of Experts has also acted as custom shaper. The International Group of Experts' thorough distillation of how existing international legal provisions apply to cyberoperations has helped focus debates and structure governmental legal positions. Custom catalysts/shapers have the capacity to make referent parties (i.e. states) develop their positions and legal views on emerging policy matters, and can help build momentum and

---

445 Expert #9, Interview #9 (2019).

446 Gary Corn, Tallinn Manual 2.0 – Advancing the Conversation (2017) ⟨https://perma.cc/2ZR9-54FX⟩ accessed 29 August 2020.

447 Robert E Barnsby and Shane R Reeves, 'Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter' (2017) 95(7) Texas Law Review ⟨https://perma.cc/H3KQ-Z728⟩, 1529-1530.

create (policy) urgency.[448] They shape the contexts and processes through which referent parties reach decisions, by framing tasks and questions, assembling and engaging with relevant stakeholders, as well as 'informing ... contextual pressures and interests'.[449]

The two International Groups of Experts, and the second Group even more noticeably so, have prompted governmental actors to 'engage in legal positioning'.[450]

> The Tallinn processes have – and have intentionally – impelled states to engage in a rule-definition process on the terms and timing of the Tallinn expert-led groups. And those terms and timing included tackling a first-stage, law-of-war-driven project, Tallinn 1.0, before taking on the broader process of Tallinn 2.0.[451]

In support of these statements, recent years have seen increasing numbers of public attribution claims being issued by states. Governments have begun to set out particular views on how international legal regimes apply to the virtual realm. In a letter to the President of the House of Representatives, the Dutch Minister of Foreign Affairs, for example, delineated the country's view on the obligations of governments apropos sovereignty, non-intervention, the use of force, due diligence, international humanitarian and human rights law, as well as attribution of and options for responding to malicious cyberoperations.[452] The latter as well as the accompanying appendix made explicit reference to the Tallinn Manual 2.0 and specific rules contained therein, including Rule 4 concerning the violation of sovereignty (a state must not conduct cyberoperations that violate the sovereignty of another state).[453]

---

448 Ingber (n 436).

449 Ibid 1546.

450 Ibid 1547.

451 Ibid 1547.

452 Michael N Schmitt, The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis (2019) ⟨https://perma.cc/6AN7-BKN6⟩ accessed 29 August 2020; Ministry of Foreign Affairs of the Netherlands, Letter to the Parliament on the International Legal Order in Cyberspace (2019) ⟨https://perma.cc/Q7D5-XUCZ⟩ accessed 29 August 2020.

453 Apropos Rule 4, for instance, the letter held that '[i]n general the government endorses Rule 4,

The French Ministry of Defence has also added to the growing body of opinio juris, one of the key elements of customary international law, on the application of international legal provisions in cyberspace. In a 20-page document on *International Law Applicable to Operations in Cyberspace* (Droit international appliqué aux operations dans le cyberespace), the French Ministry of Defence, among other things, maintained that

> [t]he international norms and principles that flow from State sovereignty apply to the use of ICT by States and to their territorial jurisdiction over ICT infrastructure. ... The principle of sovereignty applies to cyberspace. France exercises its sovereignty over the information systems located on its territory. The gravity of a breach of sovereignty will be assessed on a case-by-case basis in accordance with French cyberdefence governance arrangements in order to determine possible responses in compliance with international law.[454]

This interpretation of sovereignty as a baseline rule in the virtual realm is in line with the expert opinions voiced in the Tallinn Manual 2.0, and also the position laid out by the Dutch Minister of Foreign Affairs. As part of an introductory paragraph, the French Ministry of Defence further recognised

> the work in this sphere currently being carried out by academics and independent experts, of which the Tallinn Manual 2.0 is the most comprehensive example to date. Although the Tallinn Manual's authority is closely linked to that of the experts to whom it owes its publication, it can nonetheless stimulate international thinking on the international law applicable to cyberoperations.[455]

Rather than on areas of alignment, however, the French position paper, when making references to the Tallinn Manual 2.0, mainly focused on points of interpretive divergence

---

proposed by the drafters of the Tallinn Manual 2.0, on establishing the boundaries of sovereignty in cyberspace. Under this rule, a violation of sovereignty is deemed to occur if there is 1) infringement upon the target State's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state. The precise interpretation of these factors is a matter of debate', see Letter to the Parliament on the International Legal Order in Cyberspace (n 452).

454 Ministère des Armées, *International Law Applied to Operations in Cyberspace* (techspace rep, 2019) ⟨https://perma.cc/K65Z-9E8V⟩ 6-7.

455 Ibid 5.

from the Manual.[456]

In addition to its role as custom shaper, the International Group of Experts has further acted as discussion feeder/gap filler. In the absence of comprehensive instances of state practice and opinion juris on how international legal regimes regulate nefarious cyberactivities, the International Group of Experts has provided content for debate/analysis and has offered interpretative stepping stones. As per Schmitt, the cyberattacks on Estonia and Georgia in 2007 and 2008, respectively, made evident that guidance on how to respond to nefarious cyberoperations was in short supply.

> To address the analytical void, the then-newly established NATO Cooperative Cyber Defence Centre of Excellence, based in Tallinn, launched a multiyear project to assess the cyber relevance of the international law governing situations involving the use of force, ... as well as the applicability of international humanitarian law to cyber operations during armed conflicts.[457]

Other members of the legal community have recognised that

> there is increasing collaboration between international lawyers from around the world to help develop effective and practical standards by which states should conduct their activities in cyberspace, both through articulating the rules of international law and pushing for progress in states reaching agreement on them.[458]

Although critical of the efforts undertaken by the International Group of Experts, legal scholars including Dan Efrony and Yuval Shany, have acknowledged that Tallinn Manual contributors have executed gap-filling functions. Specifically, they argued that

---

[456] For instance, the French paper noted that '[c]ontrary to the Tallinn Manual, France considers that an attack within the meaning of Article 49 of AP [(Additional Protocol)] I may occur even if there is no human injury or loss of life, or physical damage to goods. Thus, a cyberoperation constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required in order to restore the infrastructure or the system', see Ministère des Armées (n 454) 13.

[457] Michael N Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum' (2017) 8 Harvard National Security Journal ⟨https://perma.cc/5GVK-NLT6⟩.

[458] Harriet Moynihan, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace' [2020] Journal of Cyber Policy 1 ⟨https://perma.cc/94ZW-86WT⟩, 14.

> [t]he approach taken by the Tallinn Rules drafters – to extend the analogy to existing law – as far as possible has the advantage of avoiding a regulatory void. However, it does expose the rules, and subsequent attempts to regulate the field on their basis, to academic criticism and puts them under growing pressure the more State practice deviates from them because of gaps between international law and what they consider to be their national security interests.[459]

4.2.5 Effectiveness Review: Building Ground

With reference to the drafters' intentions, i.e. to provide governmental legal advisers, who in turn guide the opinions of policymakers, with comprehensive examinations of how existing international legal provisions apply to cyberoperations in peacetime and in war, assessments of success concerning stated intentions are important elements for estimating the Group's value and long-term potential to inform normative structures in cyberspace.

With this in mind, this section evaluates the Group's contributions to cybersecurity norm formation processes along the three effectiveness dimensions introduced earlier, and rates them as low, medium, or high.

Output

The two international Groups of Experts have each produced comprehensive compendia of how international legal norms, in particular the bodies of jus ad bellum and jus in bello, translate to the virtual realm. Comprising almost 600 pages, the Tallinn Manual 2.0 has come to constitute 'the most comprehensive analysis of how existing international law applies to cyberoperations', listing relevant rules as well as consenting and dissenting expert opinions.[460] Both in the run-up to the finalisation of the second Manual as well as subsequent to its publication, individual members of the Group have

---

[459] Efrony and Shany (n 150) 59.

[460] Factsheet: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (n 158).

engaged in concerted promotion efforts, and presented the contents of their year-long deliberations at events, conferences, specialised processes (e.g. the Hague Process), in journal articles, as well as online.[461] What is more, the Manuals' editors have used their acquired expertise and know-how to found a spin-off company, Cyber Law International, which applies and disseminates the contents of the Tallinn Manuals.[462] Cyber Law International is a boutique international law firm which offers training courses on how international law applies to cyberspace for state legal advisers and other interested parties, including research institutes such as the Geneva Centre for Security Policy.[463]

In terms of substantive provisions analysed and commentaries produced, no other non-state actor surveyed as part of this thesis has issued comparable amounts of work in the context of promoting stability and security in cyberspace. Based on the premise that international legal stipulations apply to cyberspace, the second International Group of Experts has offered comprehensive interpretations of the pillars of responsible behaviour in cyberspace. Hence, in terms of output, the second International Group of Experts has demonstrated high levels of effectiveness.

Outcome

In line with what has been mentioned earlier, the second edition of the Tallinn Manual has been widely cited and commented on, whereby references have ranged from statements of endorsement to declarations of reservation.[464] In terms of effects on target

---

461 Tallinn Manual 2.0 – Advancing the Conversation (n 446); Michael Schmitt and Liis Vihul, International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms (2017) ⟨https://perma.cc/ALK4-EGDN⟩ accessed 5 September 2020; Michael N Schmitt, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty' (2019) 126 Harvard Law Review Forum 176 ⟨https://perma.cc/82FR-TA6Z⟩.

462 Cyber Law International, Cyber Law International (2020) ⟨https://perma.cc/8VNS-XXRE⟩ accessed 5 September 2020.

463 Ibid.

464 Jensen (n 422); Efrony and Shany (n 150); Kubo Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 American Journal of International Law 81; Nicholas Tsagourias, 'The Slow Process of Normativizing Cyberspace' (2019) 113 AJIL Unbound 71 ⟨https://perma.cc/4TGK-WQJN⟩.

audiences (outcome), opinions of commentators about the contributions of the Tallinn Manual 2.0 have varied. Efrony and Shany in their seminal article entitled *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, for instance, have alleged that the Manual's bearings on government postures have been minimal, in the sense that the Manual is tucked away on a book shelf, and is not resorted to frequently and thus without greater effects. Specifically, they have contended that

> the Rules' impact on state practice and whether they consider the Rules as an acceptable basis for governing cyberoperations remains unclear due to the persistent policy of silence and ambiguity relied on by many states, as well as because of practical problems relating to the application of international law to cyberspace and ongoing challenges to the contents and authority of the Tallinn Rule[s].[465]

While consistent demonstrations of state practice and opinio juris have been rare occasions, generally speaking, since 2018 several states (primarily of Western origin) have become more expressive about how they consider international law to apply in cyberspace, and in their explanations have made explicit references (either in alignment with or in opposition) to the Tallinn Rules.[466] Cognisant of these developments, this thesis views the contributions made by the second International Group of Experts more favourably than Efrony and Shany. In terms of outcome, the work undertaken by the second International Group of Experts has made governmental actors 'engage in legal positioning' and contextualisation, and has introduced behavioural points of reference.[467] Although arguments around state-driven pursuits of *policies of optionality* are hard to dismiss, i.e. arguments which hold that governments treat the application of international legal standards as optional whenever favourable to them, the Tallinn

---

[465] Efrony and Shany (n 150) 588.

[466] Jeremy Wright, Cyber and International Law in the 21st Century (2018) ⟨https://perma.cc/JT3C-JZP8⟩ accessed 28 May 2018; Ministère des Armées (n 454); Letter to the Parliament on the International Legal Order in Cyberspace (n 452); Kersti Kaljulaid, President of the Republic at the Opening of CyCon 2019 (2019) ⟨https://perma.cc/7Y2Z-M6UP⟩ accessed 8 September 2020.

[467] Ingber (n 436) 1547.

Manual 2.0 has provided governments with learning and engagement opportunities, and has *triggered* (emphasis added) responses and reactions.[468] In concurrence with Mačák '[i]t is these reactions that then become building blocks in the edifice of emerging rules of custom and interpretations of treaty rules — in other words, the law'.[469] Hence, in terms of outcome effectiveness the efforts conducted by the second International Group of Experts have shown fair results (at the very least).

Impact

In light of the hesitation and ambiguity displayed by the majority of governments across the world vis-à-vis accepting or invoking 'the normative categories used in the Tallinn Rules – armed attack, use of force, violations of sovereignty, and violations of due diligence obligations – to draw meaningful legal distinctions in their reactions to cyberoperations', it is hard to argue that the labours of the second International Group of Experts have had far-reaching systemic effects.[470] Furthermore, as is true for most of the case studies surveyed as part of this thesis, global levels of cybersecurity have not directly increased as a result of the rules issued by the two International Groups of Experts (at least not statistically). On the contrary, nation state-level cyberattacks have been increasing over the course of the last five years.[471]

Irrespective of these developments, however, the rules contained in the Tallinn Manual 2.0 have provided solid bases around which normative discussions can be held. Even in cases of contentious debates or disapproving standpoints, they offer useful

---

468 Efrony and Shany (n 150); Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (n 464) 648.

469 Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (n 464) 85.

470 Efrony and Shany (n 150) 654.

471 Craig Hinkley, Nation-State Cyberattacks: It's Bigger Than Iran (2020) ⟨https://perma.cc/2EJH-ATQN⟩ accessed 9 September 2020; Anthony Galloway, Cyber Attacks from State-Based Actor Increasing (2020) ⟨https://perma.cc/3LJK-KD5F⟩ accessed 9 September 2020.

preliminary discursive building blocks which have the potential to inspire customary standards of responsible behaviour and treaty interpretation in cyberspace, and be of systemic relevance.[472] With regard to the criticism voiced by Efrony and Shany, i.e. that governments display little inclination to rely on the Tallinn Rules and that the Manual merely sits on the shelves of legal advisers, it is useful to note that 'the fact that a compilation of rules like the Tallinn Manual sits *on the shelves* of legal advisers around the world should not necessarily be seen as a weakness'.[473] Analogising the written works drafted by the International Group of Experts to cookbooks, Mačák, for instance, aptly maintained that

> one [does not] really have to keep the cookbooks on the kitchen stove for them to have an impact on one's gastronomical creations. As long as the chef takes them *off the shelf* here and there and peruses them before beginning the next cooking adventure, they will probably have some influence on what the guests will consume that night. Like cookbooks, rule books (and other norms proposals) actually belong on the shelves – what matters is that they are easy to reach.[474]

While contested in terms of legal status, the contents contained in the Tallinn Manual 2.0 may prove to be important determinants for the emergence of international customary standards pertaining to cybersecurity. According to traditional notions of customary international law, binding habitus requires the presence of two elements: (a) consistent state practice and (b) opinio juris.[475] Although the practices advanced by non-state actors in the context of international peace and security in cyberspace fit only imperfectly into conventional frameworks of customary international law (as they

---

[472] Efrony and Shany (n 150).

[473] Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (n 464) 86.

[474] Ibid 86.

[475] Wex Legal Dictionary, Opinio Juris (2018) ⟨https://perma.cc/WTV6-YNJD⟩ accessed 23 October 2018.

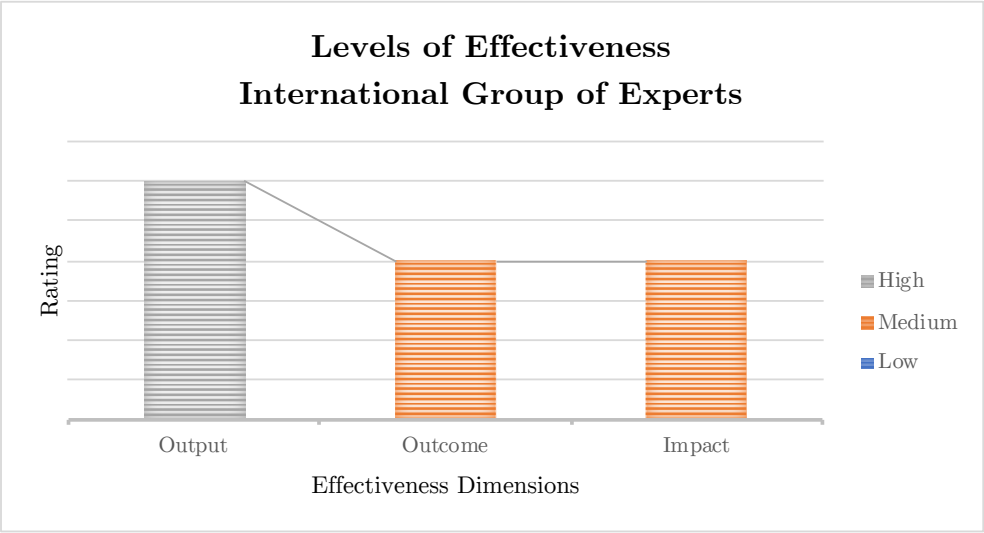

Figure 4.2: Effectiveness Plot: Second International Group of Experts.

are not state-driven), their law-like normative and custom-inspiring effects should not be discounted.[476]

Paying due regard to the remarks above, the efforts conducted by the second International Group of Experts have shown medium levels of impact effectiveness.

4.2.6 Précis

This section has analysed the activities undertaken by the second International Group of Experts vis-à-vis promoting peace and stability in the virtual realm. The examinations have revealed that in the context of forming rules of the road for cyberspace, the drafters of the Tallinn Manual 2.0 have taken on key roles as knowledge brokers, custom sharpers, and discussion feeders. They have offered rich interpretations of how existing international legal provisions apply to the digital realm, have furthered

[476] Jacqueline Eggenschwiler and Joanna Kulesza, 'Non-State Actors as Shapers of Customary Standards of Responsible Behaviour in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020).

deliberations about rules of the road for cyberspace, and have submitted normative baselines related to international law.

	Output	**Outcome**	**Impact**
High	The second International Group of Experts has issued comprehensive interpretations of the key pillars of responsible behaviour in cyberspace.	-	-
Medium	-	The work undertaken by the second International Group of Experts has made governmental actors engage in legal positioning and contextualisation, and has introduced behavioural points of reference.	The rules contained in the Tallinn Manual 2.0 have provided solid bases around which normative discussions can be held. They offer useful preliminary discursive building blocks which have the potential to inspire customary standards of responsible behaviour.
Low	-	-	-

Table 4.2: Effectiveness Review: Second International Group of Experts.

Though extensive, the endeavours of the second International Group of Experts have had mixed effects on third parties and systemic conditions. With a view to maintaining room for strategic manoeuvres, states have been hesitant to subscribe to the normative prescriptions contained in the Tallinn Manual 2.0 and to rely on the interpretations offered by the experts as part of their practices in cyberspace. Consequently, vis-à-vis outcome and impact the efforts pursued by the second International Group of Experts have only shown medium levels of success. In congruence with what has been noted by Jensen, the publication of the Tallinn Manual 2.0 has constituted only the beginning of a longer journey, which will (have to) take place over the course of 'the next several years

and perhaps longer'.[477] The activities pursued by the drafters, have, however, already operated as norm-making incubators, and have 'contribute[d] in important ways to the pluralisation of international norm-making'.[478] Customary interactions never emerge instantaneously or fully formed. Rather, they are the products of repeated exchanges across different institutional contexts and among different entities over time.[479] As many regulatory functions are increasingly constituted and performed outside entirely governmental structures, the norm-stipulating activities of private protagonists can serve as important precedents for customary principles.[480]

Furthermore, in evaluating the efforts undertaken by the second International Group of Experts, it useful to reflect on some of the advantages of non-state-actor-driven/soft law processes. In the remit of promoting rules of the road for cyberspace, there is

> a focus on practical, operational rules and on how to employ them. There is a focus on states and what states will be willing to accept and implement, as well as useful – and to some degree unique – levels of engagement between scholars and practitioners working in this realm. The combination of practicality and engagement gives these experts added legitimacy in seeking to constrain state actors.[481]

Attempts by non-state actors to inspire and evaluate the application of rules of the road for policy contexts which some experts have deemed ungovernable serve as important accelerators for otherwise even more protracted rule-making processes.

---

[477] Jensen (n 422) 778.

[478] Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (n 464) 85.

[479] Finnemore and Hollis (n 45); Eggenschwiler and Kulesza (n 476).

[480] Eggenschwiler and Kulesza (n 476).

[481] Ingber (n 436) 1554.

4.3 The Hague Program for Cyber Norms: Sustaining International Processes

Academic institutions as well as individual researchers have been decisive for the development, architectural and normative design, as well as the expansion of the virtual realm.[482] To illustrate, the progenitor of the modern internet, a network called ARPANET (Advanced Research Projects Agency Network), initially connected mainframes at four academic institutions, including the University of California, Los Angeles; Stanford University; the University of California, Santa Barbara; and the University of Utah, before eventually expanding to other entities. Institutions of higher education have been critical as well in terms of identifying, classifying, documenting, and mitigating threats emanating from networked ICTs.[483] In addition, they have contributed to track 1.5 and track 2 dialogues, and have informed 'government thinking and position development ahead of negotiations' through diligent and policy-near research outputs. These semi-formal and informal policy spaces supported by academic institutions have been seen to provide useful vehicles for bridging intergovernmental discussion-deadlocks and providing 'discrete (and plausibly deniable) venues for building confidence, facilitating exchanges on sensitive issues relating to doctrine and strategy', as well as establishing baselines for potential events of escalation.[484]

In the context of rules of the road for cyberspace, current and past examples of such efforts have included the *Harvard, MIT and University of Toronto Cyber Norms*

---

[482] Radu (n 35); Shackelford (n 35); 30 Years of TCP and IP on Everything (n 35); Leiner and others (n 35).

[483] For instance, *Citizen Lab*, an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy at the University of Toronto, has investigated acts of digital espionage against civil society organisations, documented civil rights-infringing filtering practices, and analysed information, security and privacy controls of widely-used applications, among other things, see Citizen Lab, About the Citizen Lab (2020) ⟨https://perma.cc/F2VE-VH7H⟩ accessed 29 August 2020.

[484] Cornish and Kavanagh (n 356) 18.

Workshop, as well as the *Hague Program for Cyber Norms*, the latter of which will be analysed in greater detail below.[485]

4.3.1 Background: Prioritising Norms-Oriented Research

Inaugurated in 2016, the *Hague Program for Cyber Norms* is an 'independent and inclusive platform', which seeks to advance the development and implementation of norms of responsible behaviour in cyberspace. Formally associated with the Institute of Security and Global Affairs at Leiden University's Faculty of Governance and Global Affairs, the Program applies critical thinking to problems concerning peace and stability in the virtual realm, and provides a space for governmental and non-governmental entities to exchange views on pertinent cybersecurity policy issues.[486]

The Hague Program for Cyber Norms was established with funding granted by the Dutch Ministry of Foreign Affairs, and constitutes part of the country's broader norms-oriented engagement strategy, rolled-out in the aftermath of fourth Global Conference on Cyberspace (GCCS) held in The Hague in 2015. Since its inauguration, the Program has expanded in size, and has come to comprise ten contributors, most of whom have a formal affiliation with the Institute of Security and Global Affairs (as at May 2020).[487]

4.3.2 Mandate and Goals: Furthering Norm Formation

As part of its overarching mandate to further the formation and implementation of rules of the road for cyberspace, the Hague Program for Cyber Norms has pursued different research avenues. While its initial efforts were closely tied to questions

---

485 Hurwitz, *An Augmented Summary of the Harvard , MIT and University of Toronto Cyber Norms Workshop* (n 199); The Hague Program for Cyber Norms, Hague Program for Cyber Norms (2020) ⟨https://perma.cc/J2GE-7UMM⟩ accessed 29 August 2020.

486 Hague Program for Cyber Norms (n 485).

487 ibid. In addition to its permanent body of contributors, the Program also hosts short-term visiting fellows active in research areas associated with cybersecurity norms, who want to draw on the Program's expertise, and at the same time promote their own research.

around the implementation of the eleven norms adopted as part of the 2015 UN GGE recommendations on responsible state behaviour in cyberspace, its recent endeavours have been concerned with topics including the functions of non-traditional norm-setters, as well as processes of assigning responsibility for malicious activities in cyberspace (attribution).[488]

With a view to disseminating normative thought leadership and fostering multistakeholder-based interactions about shared standards of responsible conduct in cyberspace, the Hague Program for Cyber Norms has actively participated in events and conferences hosted by other stakeholders interested in similar topics. For instance, in the remit of the 2019 *CYBERSEC Brussels Leaders' Foresight* meeting, the Program's Senior Fellow, Dennis Broeders, took part in a *VIP Working Dinner on Cyber Norms*, titled 'Paris Call, What Next?', which discussed the state of play of cybersecurity norms and possible next developments.[489]

4.3.3 Activities: Developing Concepts

As an academic research platform dedicated to 'studying what is happening in the digital world and building up knowledge about cyber[security] norms', the centre has established a diverse portfolio of research outputs. In addition to norms-related single-author journal publications, the Hague Program for Cyber Norms has published several working papers and policy reports in collaboration with international, non-governmental partner institutions, including ICT4Peace and EU Cyber Direct.[490]

---

488 The Hague Program for Cyber Norms, Research and Publications (2020) ⟨https://perma.cc/EM9N-6UDV⟩ accessed 29 August 2020.

489 The Hague Program for Cyber Norms, Dennis Broeders at Working Dinner on Cyber Norms Paris Call, What Next? (2019) ⟨https://perma.cc/U63K-E3DX⟩ accessed 29 August 2020.

490 Research and Publications (n 488). EU Cyber Direct is a multi-year project funded by the European Union, which supports the latter's diplomatic efforts pertaining to cyberspace, and facilitates exchanges among 'governments and non-governmental actors to explore ... issues surrounding international law in cyberspace, norms of responsible state behaviour and confidence building measures', see EU Cyber Direct, European Union Institute for Security Studies (2020)

One of the research outputs which has received considerable attention, and has transpired beyond academic confines is Senior Fellow, Dennis Broeders' pitch for a norm for the protection of the public core of the internet.[491] Dennis Broeders' proposal has inter alia been taken up and further promoted in expert reports and regulatory texts, such as the GCSC's final report, the EU Cybersecurity Act, or the Paris Call for Trust and Security in Cyberspace.[492] The proposed norm requires states to refrain from unwarrantedly interfering with the public core of the internet, which includes its main protocols and infrastructures.[493]

As per the author, the public core

> does not comprise the whole of the internet or even enter into the content layer of the internet but is limited to the logical and physical infrastructural layers of the core internet. It is deliberately a *lowest common denominator approach* that aims to keep the concept of the public core close to the minimum that is needed to protect the functionality of the internet.[494]

The norm's appeal and pull are based on the presumption that, given nations' shared levels of dependency on working digital infrastructures for delivering economic,

---

⟨https://perma.cc/97DX-DQ99⟩ accessed 29 August 2020. ICT4Peace, in turn, is a Geneva-based, international policy foundation, which aspires to 'save lives and protect human dignity through [ICTs]', see ICT4Peace Foundation, Mission (2020) ⟨https://perma.cc/B6UG-PFSG⟩ accessed 29 August 2020.

491 Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (The Netherlands Scientific Council for Government Policy ed, Amsterdam University Press 2016) ⟨https://perma.cc/S4NN-LEDQ⟩.

492 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (techspace rep, 2019) ⟨https://perma.cc/7FEY-3VB2⟩; Global Commission on the Stability of Cyberspace, European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act (2019) ⟨https://perma.cc/YA4C-L6P5⟩ accessed 25 August 2019; European Union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation' [2019] (L151/15) Official Journal of the European Union 15 ⟨https://perma.cc/6ZG3-SCJW⟩; Paris Call for Trust and Security in Cyberspace, Paris Call for Trust and Security in Cyberspace (2019) ⟨https://perma.cc/5XSD-5HGV⟩ accessed 5 March 2020.

493 Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (n 491).

494 Dennis Broeders, *Defining the Protection of the Public Core of the Internet as a National Interest* (techspace rep, 190, ORF Issue Brief 2017).

political, and social services, and resulting levels of digital exposure, they all share an interest in overcoming political differences and 'safeguarding the integrity and functionality of the core internet'.[495]

In addition to research publications, the Hague Program for Cyber Norms has convened two academic conferences (as at May 2020), which have brought together academic researchers, policymakers, and business representatives from different walks of life and disciplines to discuss matters pertaining to rules of the road for cyberspace over the course of several days.

The first conference, organised under the header *Responsible Behaviour in Cyberspace: Novel Horizons*, took place in the Hague in 2018, and looked at responsible state and non-state behaviour in cyberspace from multiple (and multidisciplinary) perspectives. The conference was structured around four keynote sessions, and five panel tracks on state and non-state/industry actors, power dynamics, institutional perspectives, regional perspectives and international law. The list of speakers and participants figured leading academics as well as policy and business experts in the areas of cybersecurity and internet governance.[496] In addition to the keynote and panel sessions, conference participants were given the opportunity to attend a special event at the Peace Palace during which Brad Smith, Chief Legal Counsel and President of Microsoft, delivered a talk about *Digital Peace in an Age of Cyber Threats* and

---

[495] Broeders, *Defining the Protection of the Public Core of the Internet as a National Interest* (n 494).

[496] Among others, the list of eminent speakers included Laura DeNardis (Professor and Interim Dean of the School of Communication at American University, Washington DC), Myriam Dunn Cavelty (Deputy for Research and Teaching at the Center for Security Studies (CSS) and Senior Lecturer for Security Politics at ETH Zurich), Adam Segal (Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations), Dennis Broeders, Lousewies van der Laan (former Board Member of the Internet Corporation for Assigned Names and Numbers), as well as Christopher Painter (former Coordinator for Cyber Issues for the US State Department and Commissioner for the Global Commission for the Stability of Cyberspace).

Microsoft's norms-based initiatives more generally, ahead of the unveiling of the Paris Call for Trust and Security in Cyberspace on 12 November 2018.[497]

The second conference took place a year later and followed a similar structure. Topically more narrow in scope, the second iteration of the meeting examined questions of uncertainty. Conceptualising norms of responsible behaviour as tools for managing conditions of uncertainty in cyberspace (e.g. varying levels of exposure to ICT-related vulnerabilities), it called for submissions dealing with sources of uncertainty, ways of addressing ambiguity, and goals of reducing uncertainty.[498] The second conference featured an equally esteemed list of speakers, and diverse collection of participants.[499] Among others, the group of participants included diplomatic envoys from the Asia-Pacific region for whom the conference represented an important platform for exchange, and opportunity for acquiring insights on the latest academic developments relating to rules of the road for the virtual realm, as well as peer-reviewed research in the fields of cybersecurity and international stability.

4.3.4 Role Profiles: Asking Questions and Delivering Answers

Commensurate with its academic roots, the Hague Program for Cyber Norms has acted as a well-regarded broker of information and insights across various fora and channels. In keeping with its ambitions to 'examine how consensus is developing, among governments, academics and ... society, on certain norms and how they should apply to

---

497 The Hague Program for Cyber Norms, Dennis Broeders in Q&A and Discussion with Microsoft Global President and Chief Legal Counsel Brad Smith (2018) ⟨https://perma.cc/7C8J-78RV⟩ accessed 29 August 2020.

498 Cognizant of uncertainty-inducing vulnerabilities emerging from digital technologies, key questions included: How can states, companies and citizens deal with uncertainty? How can public instruments such as (international) law, norms and confidence building measures (CBMs) but also private instruments such as insurance, liabilities and (technical) standards contribute to reducing and/or dealing with uncertainty?, see The Hague Program for Cyber Norms, 2019 Conference on Cyber Norms: Dealing with Uncertainty (2019) ⟨https://perma.cc/9XT4-YL92⟩ accessed 29 August 2020.

499 ibid. For a list of keynote speakers, please refer to: ibid.

State behaviour in cyberspace', the Hague Program for Cyber Norms has established an international platform for policy-oriented cybersecurity norms research.[500] As per Expert #29, the Hague Program for Cyber Norms has sought to engage in 'agenda setting, and creating ... a hub, internationally. I.e., where, ... people will automatically associate the cybernorms debate with ... [the] Program. So, it is [both] networking as well as agenda setting'.[501] According to Bandola-Gill and Lyall, knowledge brokering has been seen to occur across all stages of policy development, i.e. from agenda setting to evaluation.[502]

Against the background of increasingly high levels of complexity surrounding debates about rules of the road for the virtual realm, the Hague Program for Cyber Norms has offered policymakers in search of enhancing the 'use of research in policy formulation in the form of evidence-based or evidence-informed policy' rich opportunities for multistakeholder-oriented exchanges and knowledge-sharing.[503] The Program's annual conferences as well as its participation in other fora have been critical in terms of disseminating research findings, and engaging with international thinkers and practitioners. The Hague Program for Cyber Norms has actively conducted what Bandola-Gill and Lyall have referred to as 'boundary work', i.e. the crossing of different frontiers and transportation of knowledge across different stakeholder groups.[504] Knowledge brokers have been seen to translate across and coordinate

---

500 Leiden University, The Hague Program for Cyber Norms (2020) ⟨https://perma.cc/D9M6-ZC6B⟩ accessed 29 August 2020.

501 Expert #29, Interview #29 (2019).

502 Bandola-Gill and Lyall (n 441).

503 Ibid 249.

504 ibid 255. With regards to knowledge brokers, Quarmby has aptly noted that while policymakers seek for 'timely, practical input into policy matters', academics are more concerned with longer-term evaluations of pertinent policy issues. These incongruities in approaches have revealed a 'need for intermediaries who are sympathetic towards both cultures and can mediate to best effect', i.e. knowledge brokers, see Sarah Quarmby, Evidence-Informed Policymaking: Does Knowledge Brokering Work? (2018) ⟨https://perma.cc/YX5J-BQDB⟩ accessed 29 August 2020.

between different arenas, e.g. science and policy, by creating *boundary objects* relevant to the respective contexts.[505]

> Examples of boundary objects produced by knowledge brokers include conferences, reports, and research summaries. Boundary objects are characterised by two main attributes: their flexibility which makes it possible for actors from both sides of the boundary to use them for different purposes; but also their robustness, which allows the objects to maintain their identity across these different settings.[506]

The Program's boundary work has gone hand in hand with generating links and coordinating relationships between different actors. For instance, the Program's efforts surrounding the protection of the public core of the internet have served as important vehicles for strengthening 'interpersonal contacts and communication between different actors' and the Program, including between large international corporate actors, such as Microsoft and political and multistakeholder entities, such as the French Ministry of Foreign Affairs or the Global Commission on the Stability of Cyberspace.[507] Creating relationships with and among these different actors has helped the Hague Program for Cyber Norms build trust across different stakeholder communities and position itself as a responsible brokering entity.

Besides its knowledge brokering role, the Hague Program for Cyber Norms has also acted as discussion feeder. Discussion feeders are entities who provide content to and amplify policy debates (both extant and new) around urgent issues. They stimulate conversations and deliver information with a view to continuing and augmenting discursive baselines. To do so, they use different tools, including, among others, arranging thematic meetings, carrying out evaluations, or publishing policy reports, and

---

505 Bandola-Gill and Lyall (n 441).

506 Ibid 256.

507 As per Bandola-Gill and Lyall, the linking activities conducted by knowledge brokers are best understood in terms of a spectrum: 'on one end, knowledge brokers simply create connections between different actors, and on the more active end, knowledge brokers play the role of translators, mediating research between different disciplines and engaging different actors', see ibid 256.

releasing concrete proposals and recommendations. With regard to the Hague Program for Cyber Norms, the publication of a commentary pertaining to the implementation of the *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology* stipulated as part of the 2015 UN GGE report, has constituted one of its early discussion-feeding efforts. Published in late 2017, the commentary reflected the synthesised views and guidance of over 40 scholars, experts and enthusiasts on how best to implement the normative recommendations contained in the 2015 UN GGE report. The publication gained particular validity in the wake of the non-agreement outcome of the 2016-2017 UN GGE. As UN GGE members were unable to produce a consensus document, the Program's commentary offered consolidated visions on how to build on existing achievements and attain further progress.[508]

On top of the above, the Program has also actively contributed to debates about additional rules of the road for cyberspace. Specifically, it has successfully placed the concept of the protection of the public core of the internet, as developed by the Program's Senior Fellow, Dennis Broeders, across various international venues.[509] As an entity funded by the Dutch Ministry of Foreign Affairs, the Program's discussion-feeding activities can usefully be contextualised within the country's overall strong commitment to creating rules of the road for cyberspace.[510] The Netherlands has been an active contributor to international norm formation processes and has invested in different national and international platforms and coalitions, both formal and informal.[511] According to Hathaway and Spidalieri,

---

[508] Tikk and others (n 33).

[509] Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (n 491); Global Commission on the Stability of Cyberspace, *Call to Protect the Public Core of the Internet* (techspace rep, November, 2017) ⟨https://perma.cc/XY3H-MB96⟩; European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act (n 492).

[510] Hague Program for Cyber Norms (n 485).

[511] Melissa Hathaway and Francesca Spidalieri, *The Netherlands Cyber Readiness at a Glance* (techspace rep, Potomac Institute for Policy Studies 2017) ⟨https://perma.cc/DJ5N-5V9N⟩.

> [w]ith The Hague as the recognised city of international peace and security, the Netherlands aims to develop into an international centre for cyberdiplomacy that brings together international experts, policymakers, diplomats, military personnel, and NGOs in order to promote the peaceful use of cyberspace. The country is already combining knowledge from existing Dutch centres, and creating a strong network of multidisciplinary expertise to tackle different topics, such as international standards for conflict prevention, civil-military cooperation, and non-proliferation in cyberspace.[512]

The Program's debate-nurturing activities have been well-aligned with its sponsor's broader strategic policy ambitions, and have supported the government's norms-related profiling efforts across international venues including the EU, the UN, NATO, as well as Europol, and other international arenas.[513]

4.3.5 Effectiveness Review: Strengthening Discourses

In keeping with the overarching structure of this thesis, this section assesses the norm-building contributions of the Hague Program for Cyber Norms along the three dimensions of output, outcome, and impact. As has been evidenced by the preceding case studies, and will become even more apparent by the succeeding examples, the success and acceptance of norms proposals issued by non-state actors depend, among other things, on factors such as access to relevant political players and venues, standing and position, strategies of contestation, as well as proximity to dominating discourses. 'Ideas proposed by powerful non-state actors or those that are in line with dominant discourses ... are more likely to gain traction'.[514]

---

512 Hathaway and Spidalieri (n 511) 33.

513 Hathaway and Spidalieri (n 511); The Hague Program for Cyber Norms, News and Events (2020) ⟨https://perma.cc/9F8S-NNV9⟩ accessed 29 August 2020.

514 Nasiritousi (n 52) 47.

Output

Cognisant of the Program's sources of funding, in ideological terms, the research institute has been well embedded in mainstream, Western discourses about rules of the road for the virtual realm. In line with the Program's principal mission to support the adoption of normative stipulations around responsible behaviour in the digital domain and to 'apply critical thinking to cyberpeace and security issues', it has published more than a dozen research papers and edited volumes over the course of the past three years, has organised annual conferences, and has participated in various international meetings related to cybersecurity norms.[515]

In terms of output effectiveness the Program has significantly benefited from the work conducted by Senior Fellow, Dennis Broeders, and his proposal for a norm pertaining to the protection of the public core of the internet.[516] Extrapolating from the broad international uptake of Broeders' normative brain child as well as the author's concomitant policy-oriented activities clarifying his concepts and ideas, the Program's efforts vis-à-vis promoting peace and security in cyberspace have come to yield high levels of output effectiveness. The Program's capacity to appear on and present its research endeavours on international stages concerned with regulatory questions alongside large international players, such as Microsoft, also speak to the levels of normative force and cogency rendered.[517]

Outcome

With regard to outcome, the inclusion of Broeders' proposal in international policy texts issued by the Global Commission on the Stability of Cyberspace, the Paris Call initiators,

---

[515] Hague Program for Cyber Norms (n 485).

[516] Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (n 491).

[517] Dennis Broeders in Q&A and Discussion with Microsoft Global President and Chief Legal Counsel Brad Smith (n 497).

or the European Union have underscored the concept's normative value and capacity.[518] Though direct references to the norm's creator and his institutional affiliation have been sparse, the conceptual baselines cited across these texts can unmistakably be attributed to Dennis Broeders and by extension to the Hague Program for Cyber Norms.[519]

Without citing the original drafter of the norm to protect the public core of the internet, Marietje Schaake, representative of the Global Commission on the Stability of Cyberspace and former Member of the European Parliament, for instance, has argued that

> [t]]he EU's adoption of the norm to protect the public core of the Internet bears testament to the fundamental importance of this norm for enhancing stability and security in cyberspace ... . Furthermore, its inclusion in ENISA's mandate is indicative of the EU's commitment to protect the technical foundation of the open Internet, a global public good managed in a multistakeholder manner where all actors have a role.[520]

With reference to Schaake's statement it can be argued that the concept developed by Broeders has already induced acts of behavioural positioning and affected third-party postures. Overall, the Program's, and in particular Dennis Broeders', outcome-related contributions to global discussions about responsible conduct in cyberspace have been noteworthy. Appearances of government envoys and high-ranking industry representatives at the Program's annual conferences have further underscored the high levels of outcome effectiveness accomplished by the Program. Commitments of these sorts are indicative of assurances of relevance by third parties and changing, norms-oriented policy postures.

---

518 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492); European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act (n 492); European Union (n 492); Paris Call for Trust and Security in Cyberspace (n 492).

519 The Global Commission on the Stability of Cyberspace has made reference to the norm's originator in a footnote as part of its final report. The footnote held that '[a]n early proponent of identifying the public core of the Internet for special protection was Dennis Broeders, a Dutch researcher', see Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492) 20.

520 European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act (n 492).

Impact

As is often the case in security-related contexts, reliable data on the value of normative endeavours and corresponding deterrence effects are difficult to procure, let alone interpret. With regard to the activities conducted by the Hague Program for Cyber Norms it appears that technology-oriented systemic security effects have been limited, i.e. the numbers of nefarious cybersecurity operations globally have not decreased as a direct result of the project components executed by the Program. The Hague Program for Cyber Norms has however, made valuable additions to cybersecurity-relevant normative orders and has offered ideational, lowest-common-denominator building blocks around which actor expectations can converge. In addition to brokering knowledge, the Program has set off problem-solving processes which may serve as bridge-builders between and garner ideational support from diverse stakeholder groups in the long run. The broad uptake of the Program's ideas by Western-oriented stakeholder groups are early indicators of potentially more far-reaching endorsements.

Though the normative quandaries among states which, among other things, have led the creation of the Program have not abated or been resolved, the Hague Program for Cyber Norms has at least offered alternative elements for normative consensus-building and opportunities for stimulating responsible conduct in cyberspace. It has alleviated normative roadblocks and opened up alternative conceptual and discursive pathways. Although specific benchmarks or thresholds relating to levels of goal attainment have not been specified by the Program, with reference to the remarks above, it is fair to argue that in terms of impact, the Hague Program for Cyber Norms has displayed sound degrees of effectiveness.

4.3.6 Précis

As a small research-oriented platform of exchange for stakeholders from academia, industry, and government, the Hague Program for Cyber Norms has yielded sensitising

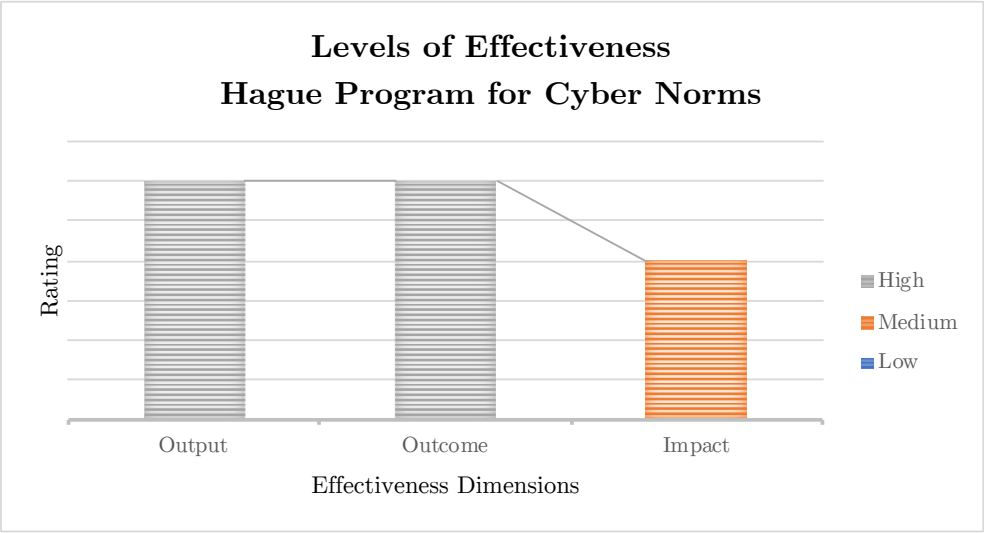

Figure 4.3: Effectiveness Plot: The Hague Program for Cyber Norms.

and substantive contributions to discussions about rules of the road for cyberspace. Following comprehensive reviews of the Program's principal activities, this thesis has maintained that the platform has executed two main roles in the context of promoting peace and security in the digital domain. For one thing, the Program has actively brokered norms-related knowledge among different stakeholders, and has hence engaged in processes of sense-making. For another, it has fed subsiding discourses about responsible conduct in cyberspace with new proposals based on the brokered understandings.

As per Bandola Gill and Lyall, the rates of success of norm-making efforts conducted by knowledge brokers are often determined by broader social, political, economic, and empirical backgrounds. Whether or not specific proposals thrive, depends among other things 'on a multiplicity of different processes and interventions'.[521] With regard to the broader contextual factors mentioned above, the Hague Program for Cyber Norms has profited from being associated with the Dutch Ministry of Foreign Affairs

[521] Bandola-Gill and Lyall (n 441) 256.

	Output	Outcome	Impact
High	The Program has appeared and presented its research endeavours on international stages concerned with regulatory questions alongside large international players, and issued concrete proposals.	The Program's proposals have already induced acts of behavioural positioning and affected third-party postures.	-
Medium	-	-	The Program has made valuable additions to cybersecurity-relevant normative orders and has offered ideational, lowest-common-denominator concepts around which actor expectations can converge.
Low	-	-	-

Table 4.3: Effectiveness Review: The Hague Program for Cyber Norms.

and the Netherlands' strategic pledges to advance the development of international norms around networked infrastructures and technologies. The endorsement by the Dutch Ministry of Foreign Affairs has strengthened the Program's international outlook and positioning as well as its access to relevant venues concerned with generating rules of the road for cyberspace.

Vis-à-vis the quality of its contributions, the efforts conducted by the Hague Program for Cyber Norms have shown high levels of output and outcome effectiveness, and medium levels of impact effectiveness. While conceptually, the Program has delivered important normative components, the ideas developed by the Program have been projected to international stages primarily through advocacy efforts pursued by other non-state actors, for instance the Global Commission on the Stability of Cyberspace or the Paris Call promoters. '[W]here states and national governments

have failed to deliver or reach consensus on certain global issues', including on the enactment of peace and security in the virtual realm, non-state actors such as the Hague Program for Cyber Norms have offered alternative proposals for convergence and participatory advancement.[522]

4.4 Stakeholder-Cluster Synthesis: Building Momentum

This chapter has examined and assessed the norm-building activities of three pertinent representatives of civil society and academia. Specifically, it has scrutinised the norm cultivation endeavours conducted by a small London-based social purpose company, *Global Partners Digital*, an esteemed group of leading academics in the field of international (cyber) law, i.e. the second *International Group of Experts*, as well as a cybernorms-dedicated research institute in the Hague, the *Hague Program for Cyber Norms*. Thematic evaluations of primary and secondary materials have revealed the following role profiles assumed by civil society and academic entities: custom shapers, awareness raisers, knowledge brokers, capacity builders, and gap fillers.

Although different in terms of origin, size, organisational focus and strategy, and even though the case studies were examined as single case studies rather than comparative case studies, the chapter has been able to identify some shared trend lines across the three cases. Not only have all the empirical examples studied as part of this chapter shown high output effectiveness, their activities, even though the three actors have executed different roles, have also displayed strong sensitising qualities. Non-state actor contributions with sensitising characteristics typically comprise elements of agenda-building, awareness-raising, and opinion-influencing. In their roles as awareness raisers and primary knowledge brokers concerning rules of the road for cyberspace, the

[522] Kavanagh and Stauffacher (n 13) 8.

three civil society and academic actors surveyed have unmistakably yielded sensitising contributions (please refer to Figure 4.4 for an overview of the different roles executed by the three civil society and academic actors).

Figure 4.4: Civil Society and Academia Contributions Spectrum.

In addition to their fairly traditional non-state actor roles as awareness raisers and translators across science and policy arenas (knowledge brokers), two of the three actors surveyed, the second International Group of Experts as well as the Hague Program for Cyber Norms, have acted as discussion feeders and custom shapers, respectively. By so doing, these actors have contributed substantive as well as context-reframing structural elements pertaining to cybersecurity norms debates. Among other things, these academic protagonists have filled substantive voids left by international policymakers, reinvigorated debates about responsible behaviour in cyberspace, and inspired legal positioning among state actors. The results of this chapter go to show that civil society and academic organisations have taken on key roles in securing and achieving

an open, secure, stable, accessible and peaceful cyberspace '(otherwise understood as a functionally reliable international ICT environment in which international law and other norms are respected)'.[523] The extensive reach of the norms-related contributions made by civil society and academic organisations has also been been evidenced in statements voiced by the experts interviewed. Experts #14, #19, #23, and #24, for instance, have all identified an intensified presence of civil society and academic protagonists across cybersecurity norms-related debates and have noted that these actors seek strategic engagement to raise awareness for specific security-related issues, including human rights and privacy. Textual artefacts such as policy papers, memos, blog posts, op-eds, or reports have further strengthened their visibility across spaces concerned with developing rules of the road for the virtual realm.[524].

All of the actors surveyed have offered rich interpretations and positions on what norms-based responsible behaviour in cyberspace looks like. They have also engaged fellow private and public entities by means of hosting workshops, attending conferences, and launching requests for input. By so doing, they have contributed to and fuelled processes of sense-making (sensitising contributions). The vast amounts of boundary objects produced by the three non-state stakeholders surveyed have also served as indicators for the high levels of output effectiveness yielded by the latter. Expert #19 has noted that non-state actors have identified

> different ways and means of engaging. And ... the engagement in comparison to, let's say, 10 years ago, when there was some activity in this area [initially], has really multiplied and the change has been quite different. Whether it is having an impact is a different question.[525]

---

[523] Geneva Dialogue, *Geneva Dialogue Final Report* (techspace rep, 2019); Kavanagh and Stauffacher (n 13) 4.

[524] Interview #14 (n 398); Expert #19, Interview #19 (2019); Expert #24, Interview #24 (2019); Interview #23 (n 399).

[525] Interview #19 (n 524).

In terms of outcome and impact, the effectiveness of the three entities have varied. As has been noted, the levels of success of norm-making efforts conducted by civil society and academic entities are frequently contingent on or at least influenced by broader social, political, economic, and empirical backgrounds. Whether or not specific endeavours thrive, depends among other things 'on a multiplicity of different processes and interventions'.[526] In terms of impact, it is useful to bear in mind that the manifestation of systemic effects may take multiple years, and may not be easily or readily identifiable. With regard to the broader contextual factors mentioned above, the Hague Program for Cyber Norms as well as the second International Group of Experts have benefited from being associated with or having well-established connections to leading government officials/ministries and being able to position their activities strategically for cross-referencing across cybersecurity norms development mechanisms. These realities are also the reasons, why in terms of outcome and impact effectiveness, the second International Group of Experts and the Hague Program for Cyber Norms respectively, have been ascribed higher ratings than Global Partners Digital.

[526] Bandola-Gill and Lyall (n 441) 256.

As member states contemplate the next steps in the development of cybernorms, the answer may be to avoid putting too much of a burden on any one institution like the UN GGE. Progress may require the simultaneous use of multiple arenas. In some cases, development of principles and practices among like-minded states can lead to norms to which others may accede at a later point. ... In other cases, such as security norms for the internet of things, the private sector, insurance companies, and non-profit stakeholders might take the lead in developing codes of conduct.

— Joseph S. Nye Jr. *How Will New Cybersecurity Norms Develop? (2018)*

5 Corporate Actors

Contents

This chapter introduces the second cluster of case studies under review. Adding to the insights gathered from examining the contributions of civil society and academia to cybersecurity norm development efforts, this chapter explores the roles assumed by corporate actors. In particular, it summarises and comments on the effectiveness of the normative strategies pursued by leading technology companies, including (a) *Microsoft*, (b) *Siemens*, and (c) *Kaspersky Lab*. For the purposes of this chapter, technology companies are understood to denote enterprises engaging in and deriving sizeable percentages of their revenues from the development, manufacturing, and maintenance of technology products and services, including, for instance, hard- and software components or platform services.

Against the background of increasing numbers of threats emanating from cyberspace targeting and involving some of the products and services offered by the companies under investigation, large-scale industry players have started to insert their voices more vocally in debates about rules of the road for the digital domain. This chapter offers details on how these companies have engaged in discussions about responsible behaviour in cyberspace, and how their (public) postures have come to resemble those of global political actors.

As regards structure, the case studies presented in this chapter follow the same organisational maxims as the case studies introduced in the previous chapter. That is, each case study starts with information about the relevant actor environments, continues with examinations of the main activities undertaken by the technology companies under investigation, before concluding with evaluations of the effectiveness of their normative efforts. In conducting the relevant case analyses, this chapter draws on concepts such as corporate norm entrepreneurship and transnational business regulation, which have tried to make sense of and explain the non-traditional, politically-inspired range of activities conducted by corporate entities.[527]

Since the early 2000s, 'there has been a burgeoning critical interest in so-called *private authority* and *private governance* at the global level'.[528] Transnational corporations (TNCs) and global business associations have been seen to execute roles conventionally ascribed to states,

> sometimes in conjunction with CSOs, but more widely on their own – ranging from instituting new accounting standards to ... various *private*

---

[527] Flohr and others, *The Role of Business in Global Governance* (n 219); Burkard Eberlein and others, 'Transnational Business Governance Interactions: Conceptualization and Framework for Analysis' (2014) 8(1) Regulation & Governance 1 ⟨https://perma.cc/U3DH-PCVD⟩. '[T]ransnational business governance (TBG) refers to systematic efforts to regulate business conduct that involve a significant degree of non-state authority in the performance of regulatory functions across national borders, see Eberlein and others (n 527) 3.'

[528] Ruggie, 'Reconstituting the Global Public Domain - Issues, Actors, and Practices' (n 51) 502.

> *regimes*, such as eco-labelling and other forms of certification designed to impress consumers with the social responsibility of participating firms.[529]

While scholars including Flohr and others have found that thrusts towards outsourcing public functions to private entities have long historical precedents, they have also noted that contrary to

> the early modern period when private actors acquired the political authority to perform state functions by formal delegation of state competencies, that is by the charters they were granted, private transnational governance contributions today mainly appear as voluntary self-commitments ... .[530]

Despite broad bodies of literatures on corporate social responsibility, norm entrepreneurship and transnational business governance (particularly in fields such as human rights and environmental studies), new governance patterns, in which transnational enterprises have come to take on 'authoritative roles and regulatory functions', have not been analysed very thoroughly in the context of cybersecurity.[531]

Non-state actors, in particular technology companies, have been key contributors to the development and expansion of cyberspace. As owners and operators of network infrastructures, designers of products, and suppliers of services, they have made important contributions to the structures and architectural features of the virtual realm.[532] In addition to producing hard- and software, and creating large-scale platforms, they have also come to contribute to the promotion of global cybersecurity norms and standards. Economically speaking, norms provide useful tools for technology companies

---

529 Ruggie, 'Reconstituting the Global Public Domain - Issues, Actors, and Practices' (n 51) 502.

530 Flohr and others, *The Role of Business in Global Governance* (n 219) 13.

531 Annegret Flohr and others, 'Variations in Corporate Norm-Entrepreneurship: Why the Home State Matters' in Morten Ougaard and Anna Leander (eds), *Business and Global Governance* (Routledge 2012) 235. See also A Claire Cutler, Virginia Haufler, and Tony Porter, *Private Authority and International Affairs* (State University of New York Press 1999); Rodney Bruce Hall and Thomas J Biersteker, *The Emergence of Private Authority in Global Governance* (Cambridge University Press 2002).

532 Radu (n 35).

to tackle contextual ambiguities and preempt costly changes to legal frameworks, or government-led market interventions. Furthermore, norms support corporate actors in sustaining their business models and executing corporate responsibility strategies.[533] And while the reasons for corporate norm-shaping efforts pertaining to the virtual realm may primarily be grounded in commercial considerations, i.e. reducing costs and risks, securing their operations, gaining access to new markets or safeguarding existing customer bases, and strengthening corporate reputation and legitimacy, less self-serving reasons, i.e. upholding good-faith-commitments and values such as user privacy and security as well as the creation of conducive (operational) ecosystems, should not be discounted.[534] Not all of the activities undertaken by technology companies in the context of norms of responsible behaviour in cyberspace can convincingly be explained by rationalist arguments but instead may also be based on underlying notions of appropriateness.[535]

5.1 Microsoft: Changing the Faces of Norm Development Processes

Founded in 1975, and employing more than 151,100 staff across 120 countries, Microsoft has emerged as one of the leading tech enterprises worldwide and has become a key contributor to discussions concerning rules of the road for cyberspace. Valued at over USD 1 trillion (as at end of 2019), it is often referred to as one of the *big five* technology giants globally, the other four being Apple, Amazon, Facebook and Alphabet (Google).

Microsoft's product offering covers a broad spectrum of items, ranging from operating systems, server and business solution applications as well as cross-device productivity

533 Expert #3, Interview #3 (2019).

534 Gorwa and Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' (n 218).

535 Ibid.

applications, to desktop and server management tools, software development tools, video games, and training and certification schemes for developers and system managers.[536] In addition to its software-oriented products, the technology heavyweight also produces and distributes hardware, including personal computers (PCs), tablets, gaming and entertainment equipment, mobile phones, and other gadgets. Microsoft also has a portfolio of services revolving around cloud-based solutions, and provides consulting and support services.[537]

Organisationally, Microsoft is divided into four engineering groups and nine business functions.[538] Most of the norms-related efforts undertaken by Microsoft (so far) have come out of the Corporate, External, and Legal Affairs function, which is headed by President and Chief Legal Officer, Brad Smith. The different groups overseen by Brad Smith

> are responsible for the company's legal work, its intellectual property portfolio, patent licensing business, corporate philanthropy, government affairs, public policy, corporate governance, and social responsibility work. His teams also lead the company's work on a number of critical issues including privacy, security, accessibility, environmental sustainability and digital inclusion, among others.[539]

5.1.1 Background: Accessing the Norms Space

Microsoft has been an early mover in terms of contributing to debates about rules of the road for cyberspace. It has been active in the norms space since at least 2013, when

---

536 Reuters, Microsoft Corporation Profile (2020) ⟨https://perma.cc/QZ4E-9CVA⟩ accessed 27 February 2020.

537 Ibid.

538 The four engineering groups consist of (a) the Cloud + AI (Artificial Intelligence) Group, (b) Experiences + Devices, (c) the Artificial Intelligence and Research team, and (d) the Core Services Engineering and Operations (CSEO) Group. The nine business functions include the Business Development Group, the Corporate, External, and Legal Affairs unit, the Corporate Strategy and Operations/Acquisitions Group, the Finance Group, Global Sales, Marketing and Operations, Human Resources, LinkedIn, the Marketing Group, and the Worldwide Commercial Business organisation, see Microsoft, Facts About Microsoft (2020) ⟨https://perma.cc/TQT2-9KFT⟩ accessed 27 February 2020.

539 Ibid.

it issued an early policy paper on *Five Principles for Shaping Cybersecurity Norms.*[540] Since then, its norms-oriented activities have proliferated substantially and have addressed different stakeholder groups, including governments, fellow industry partners, and civil society groups (please refer to Section *Activities: Engaging Extensively* for more details on the normative efforts launched by Microsoft).

As per Gorwa and Peez, Microsoft's norms-based endeavours have to be viewed (at least partly) within the context of its involvement with the United States National Security Agency's PRISM programme (2007-2013), and the resulting loss of customer trust and PR éclat ensuing the *Snowden Revelations* of 2013.[541]

5.1.2 Mandate and Goals: Targeting Diverse Stakeholders

Since 2015 Microsoft's global mission has been to 'empower every person and every organisation on the planet to achieve more'.[542] With more than 900 million devices relying on Microsoft's operating system Windows 10, customer trust has advanced to one of the company's key priorities.[543] As per Microsoft's 2019 annual report, its focus on trust

> extends to ensuring that those who use [its] products and services have confidence in the underlying technology itself. There are three pillars to [Microsoft's] approach: privacy, cybersecurity, and responsible AI. Across each, [Microsoft's] commitment goes beyond words to real actions, providing

---

[540] Microsoft, *Five Principles for Shaping Cybersecurity Norms* (techspace rep, Microsoft 2013) ⟨https://perma.cc/G6RJ-883W⟩.

[541] Gorwa and Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' (n 218). For more information on the surveillance disclosures issued by Edward Snowden, please refer to The Guardian, The NSA Files (2013) ⟨https://perma.cc/ZEC4-ZM3Q⟩ accessed 7 January 2021. See also Glenn Greenwald, Microsoft Handed the NSA Access to Encrypted Messages (2013) ⟨https://perma.cc/28BK-TPUW⟩ accessed 29 February 2020.

[542] Eugene Kim, Microsoft Has a Strange New Mission Statement (2015) ⟨https://perma.cc/Y4AN-LNN8⟩ accessed 27 February 2020.

[543] Facts About Microsoft (n 538).

> tools and frameworks for [its] customers and working collaboratively with the public sector to drive policy change.[544]

With regard to the second pillar, cybersecurity (which is of key relevance for the endeavour at hand), Microsoft has, in addition to signals analysis and authentication processing, pursued 'an ecosystem-wide approach, partnering across both the tech sector and the public sector to address new threats in an increasingly complex and heterogeneous world'.[545] In pursuit of its overarching goal to increase trust in cyberspace, it has launched a broad portfolio of norms-oriented ventures which will be dissected further in the succeeding paragraphs.

5.1.3 Activities: Engaging Extensively

One pertinent example of Microsoft's endeavours to (re)instil trust and 'promote a safe and secure digital world' in collaboration with governments, fellow technology companies, and nongovernmental organisations, has been its call for a Digital Geneva Convention.[546] Introduced by Brad Smith, at the RSA Conference in San Francisco in February 2017, Microsoft's call for a *Digital Geneva Convention* represented a response to perceived increases in nefarious (state-led) cyberattacks.[547]

Drawing analogies to the Geneva Convention (IV) relative to the *Protection of Civilian Persons in Time of War,* also known as the Fourth Geneva Convention, Smith argued that the virtual realm is in need of a digital counterpart that obliges sovereign

---

544 Microsoft, *Microsoft 2019 Annual Report* (techspace rep, 2019) ⟨https://perma.cc/55GR-AFDD⟩.

545 ibid. As per information contained in its annual report, Microsoft analyses more than 6.5 trillion signals each day, and conducts more than 400 billion email-related malware and phishing, and over 450 billion authentication checks per month, see ibid.

546 The Need For a Digital Convention (n 33).

547 Ibid.

actors to protect civilians from (state-led) malicious cyberoperations in times of peace.[548] 'And just as the Fourth Geneva Convention recognised that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies'.[549]

Met with mixed reactions form government officials and representatives of academia, the Digital Geneva Convention as sketched out by Smith called on states to (a) refrain from targeting critical (information) infrastructures, including civilian and financial systems, (b) refrain from hacking accounts of publicly exposed persons, including journalists and 'private citizens involved in electoral processes', (c) abstain from stealing intellectual property and conducting commercial espionage, (d) 'refrain from inserting or requiring backdoors in mass-market commercial technology products', (e) engage in vulnerabilities disclosure processes, (f) exercise restraint in developing cyberweapons, limit proliferation of the latter and curb offensive activities, and (g) assist private sector entities in securing cyberspace and 'enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs)'.[550] During his keynote address, Smith also floated proposals revolving around establishing an independent non-governmental organisation capable of investigating and publicly attributing (state-led) cyberattacks, analogous to the

---

548 The Need For a Digital Convention (n 33). The Fourth Geneva Convention of 1949 is concerned with the protection of civilians in times of war, armed conflict (declared or de facto), as well during times of total or partial occupation. The Geneva Conventions adopted before 1949 did not specify the regulations governing the status and treatment of protected persons but mainly focused on combatants, see International Committee of the Red Cross, Geneva Convention (IV) on Civilians, 1949 (2020) ⟨https://perma.cc/ZQ9H-ZKVY⟩ accessed 2 March 2020.

549 Microsoft, *A Digital Geneva Convention to Protect Cyberspace* (techspace rep, Microsoft Policy Papers 2017) ⟨https://perma.cc/698H-84P5⟩.

550 Microsoft, *A Digital Geneva Convention to Protect Cyberspace* (n 549); Private-Sector Initiatives for Cyber Norms: A Summary (n 216). Minárik and van der Meij for instance argued that 'calling for a Digital Geneva Convention is both legally confusing and politically unrealistic', as the Fourth Geneva Convention applies in times of armed conflict, not peacetime, and because there are existing rules states have to obey in cyberspace in peacetime, see Tomáš Minárik and Kris van der Meij, Geneva Conventions Apply to Cyberspace: No Need for a Digital Geneva Convention (2017) ⟨https://perma.cc/PR4J-P3CV⟩ accessed 2 March 2020.

IAEA, and tech companies building a neutral Digital Switzerland, which would assist 'customers everywhere and [retain] the world's trust'.[551] Both ideas have come to fruition since Smith's presentation at the 2017 RSA conference, i.e. in the form of the Cybersecurity Tech Accord and the CyberPeace Institute.[552]

14 months after Smith's introduction of the Digital Geneva Convention, Microsoft launched the Cybersecurity Tech Accord, an initiative centred around bringing together 'global technology companies committed to protecting their customers and users'.[553] From an initial 34 members, the Cybersecurity Tech Accord has grown to over 140 participants and has come to comprise signatories from areas including telecommunications, hard- and software manufacturing, endpoint protection and threat intelligence, among others.[554] As part of their commitment, members of the Cybersecurity Tech Accord have pledged to adhere to four principles, namely (a) to protect all users and customers everywhere, irrespective of size, technical acumen or location, (b) to oppose (state-led) cyberattacks on innocent citizens and businesses, regardless of culture or location, (c) to empower developers and users to protect themselves by providing information and tools and building capacity to develop security measures, and (d) to engage in collaboration and share information with fellow signatories as well as other like-minded groups, including other industry partners, civil society, and security researchers, across proprietary and open source technologies.[555] While the Cybersecurity

[551] The Need For a Digital Convention (n 33).

[552] Cybersecurity Tech Accord, Cybersecurity Tech Accord (2018) ⟨https://perma.cc/4W5G-FK3L⟩ accessed 10 July 2018; 34 Companies Stand Up for Cybersecurity with a Tech Accord (n 33); Working Towards a Safer Online World for All (n 33).

[553] Cybersecurity Tech Accord (n 552). In terms of objectives, '[s]ignatories are committed to advancing the mission of the Cybersecurity Tech Accord by partnering on initiatives that improve the security, stability, and resilience of cyberspace. By combining the resources and expertise of the global technology industry, the Cybersecurity Tech Accord creates a starting point for dialogue, discovery and decisive action', see ibid.

[554] For more detailed information pertaining to member structure and accession motivations, please refer to Gorwa and Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' (n 218).

[555] Cybersecurity Tech Accord (n 552); Private-Sector Initiatives for Cyber Norms: A Summary (n 216).

Tech Accord has been acceded to by leading S&P 500 companies including Facebook, Symantec, and Cisco Systems, it has failed to garner support from other industry heavyweights, such as Alphabet, Apple, or Amazon.[556] Moreover, despite pursuing global expansion strategies, it has not received any endorsement from corporations based in China, Israel, or Russia.[557]

As per information contained in the Cybersecurity Tech Accord's 2019 annual report and in opposition to claims that the Cybersecurity Tech Accord has mostly served PR-related purposes, members have done more than publicly issuing statements of support and signing pledges.[558] Among other things, they have conducted webinars, started to identify and implement vulnerabilities disclosure policies, phrased consultation responses, partnered with the United Nations Office of Disarmament Affairs and the United Nations Envoy on Youth to launch *Apps 4 Digital Peace*, a youth competition to improve global cybersecurity, and have been vocal advocates for multistakeholder-based efforts to strengthen peace and security online.[559]

In October 2018, Microsoft unveiled another, civil society-oriented initiative entitled *Digital Peace Now*. Supported by NGOs and think tanks, including ICT4Peace, Civicus, and Observer Research Foundation, the Digital Peace Now campaign asks members of civil society to urge 'world leaders to create a safer cyberspace' and practice cyberhygiene. To date, the Digital Peace Now petition has been signed by more than 100,000 people, across 140 nations.[560] Contrary to the two efforts introduced earlier, information and commentary pertaining to the Digital Peace Now initiative

---

556 Private-Sector Initiatives for Cyber Norms: A Summary (n 216).

557 Gorwa and Peez, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' (n 218).

558 Cybersecurity Tech Accord, *2019 Year In Review* (techspace rep, 2019) ⟨https://perma.cc/YX6V-9DLP⟩.

559 Ibid.

560 Microsoft, Digital Peace Now (2018) ⟨https://perma.cc/88RC-N8ZX⟩ accessed 4 December 2018.

have been sparse, and activities not well-publicised, which invites questions as to the initiative's status and import.

One month after the launch of its Digital Peace Now campaign, in November 2018, Microsoft postulated its support for the *Paris Call for Trust and Security in Cyberspace*.[561] Introduced at the twelfth UN Internet Governance Forum (IGF) in Paris by French President Emmanuel Macron, the Paris Call for Trust and Security in Cyberspace (short Paris Call) constitutes one of the most widely endorsed multistakeholder instruments pertaining to peace and security in the virtual realm. It proposes the development of common principles for securing cyberspace through collaborative efforts across existing international platforms and mechanisms.[562] Although at first sight a French (and government-led) initiative, the Paris Call was vitally influenced by Microsoft, both in terms of origin and content. According to information presented by Le Monde and WIRED, it was Microsoft's political lobbying that gave rise to the initiation of the Paris Call.[563]

The Paris Call as introduced by Macron advances nine high-level principles intended to resonate with both state and non-state entities. Specifically, it commits supporters to:

> Prevent and recover from malicious cyberactivities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;
>
> Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;

---

561 Brad Smith, An Important Step Toward Peace and Security in the Digital World (2018) ⟨https://perma.cc/25C9-2C82⟩ accessed 4 March 2020.

562 Ministère de l'Europe et des Affaires Étrangères, Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace (2018) ⟨https://perma.cc/8P82-X5JU⟩ accessed 10 December 2018.

563 Louise Matsakis, The US Sits Out an International Cybersecurity Agreement (2018) ⟨https://perma.cc/6F5B-V24W⟩ accessed 13 December 2018; Par Martin Untersinger, La France Veut Relancer les Négociations Sur la Paix Dans le Cyberespace (2018) ⟨https://perma.cc/FUH3-HYMV⟩ accessed 19 August 2019; Arthur PB Laudrain, Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace (2018) ⟨https://perma.cc/DD7J-JGQF⟩ accessed 5 December 2018.

> Strengthen [signatories'] capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyberactivities;
>
> Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;
>
> Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;
>
> Strengthen the security of digital processes, products and services, throughout their life cycle and supply chain;
>
> Support efforts to strengthen an advanced cyberhygiene for all actors;
>
> Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;
>
> Promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace.[564]

Rather than reinventing the wheel in terms of normative stipulations, the Paris Call constitutes an attempt at broadening support for and realigning fragmented norms-related discussions which have been scattered across multiple fora. Among other things, the Paris Call makes reference to norms developed by entities such as the UN GGEs as well as the Global Commission on the Stability of Cyberspace. For instance, principles two and seven of the Paris Call build on norms one and seven of the catalogue issued by the Global Commission on the Stability of Cyberspace.[565]

While the Paris Call has generally seen broad uptake among governments, private industry, the technical community, researchers, non-governmental organisations and civil society, there have been notable abstentions.[566] Neither the United States, nor Russia, China, Iran or Israel have publicly announced their support for the Paris Call,

---

564 Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace (n 562).

565 Global Commission on the Stability of Cyberspace, *Final Report Fact Sheet* (techspace rep, 2019) ⟨https://perma.cc/TT4W-USKU⟩.

566 Since its inauguration in November 2018, the Paris Call has doubled in size. It has come to enjoy the support of more than 1,000 signatories, including 78 governments, 29 public authorities, 343 civil society organisations, and 633 private sector entities, see Ruhl and others (n 314); Paris Call for Trust and Security in Cyberspace (n 492).

showcasing the geopolitical complexities and faultlines surrounding discussions about norms of responsible behaviour in cyberspace.[567]

With regard to fostering implementation of the principles stipulated by the Paris Call and with a view to waving off criticisms surrounding window-dressing and pretension (non-action), supporters of the Paris Call have recently proposed the launch of a *Paris Call Community* or rather different Paris Call Communities, i.e. the formation of 'different interest groups dedicated to advancing best practices and building the capacity to conform around each of the Paris Call principles'.[568] First groups, for instance on *Countering Election Interference* have already started to form.[569]

Approximately two months before the first-year anniversary of the Paris Call, in September 2019, Microsoft, in collaboration with the Hewlett Foundation, MasterCard and other contributors and partners, inaugurated the CyberPeace Institute.[570] The CyberPeace Institute was founded with the intention of enhancing the stability of the virtual realm through assistance, analysis, advancement, as well as foresight and capacity building.[571] Operationally headed by Stéphane Duguin, former Head of the EU Internet Referral Unit within Europol, and presided by Marietje Schaake, a former member of the European Parliament for The Netherlands as well as the Global Commission on the Stability of Cyberspace, the CyperPeace Institute also houses an Executive Board and Advisory Board, made up of global experts in cybersecurity, international law, human rights law and international affairs.[572]

---

567 The US Sits Out an International Cybersecurity Agreement (n 563).

568 Ruhl and others (n 314) 11.

569 John Frank, Paris Call: Growing Consensus on Cyberspace (2019) ⟨https://perma.cc/NKG2-ZDP4⟩ accessed 6 March 2020.

570 CyberPeace Institute, Partners (2020) ⟨https://perma.cc/3Y52-TV9D⟩ accessed 6 March 2020.

571 Working Towards a Safer Online World for All (n 33).

572 Maggie Miller, Microsoft, Mastercard, Hewlett Foundation Launch Institute to Investigate Cyberattacks (2019) ⟨https://perma.cc/X827-S4DG⟩ accessed 6 March 2020. For a full list of members, please consult Working Towards a Safer Online World for All (n 33).

The Institute's activities, revolve around four main pillars, namely (a) to help vulnerable communities recover from cyberattacks, and increase digital resilience (assistance), (b) to analyse in a multistakeholder-oriented fashion cybersecurity incidents with a view to determining facts and holding perpetrators to account (analysis), (c) to 'advance international law and norms in order to promote responsible behaviour in cyberspace' (advancement), and (d) to forecast and analyse emerging opportunities and risks associated with new technologies (foresight).[573]

Based in Geneva, Switzerland, the CyberPeace Institute boasts itself as an nonpartisan organisation guided by principles such as neutrality, independence, impact, transparency, integrity, as well as inclusiveness. With its mission to provide cybersecurity-related assistance, analysis/accountability, advancement, and foresight at scale, the Institute is envisaged to'fill an important unmet need, [and] joins a range of other critical work underway to help secure the internet', including the Cybersecurity Tech Accord, the Paris Call for Trust and Security in Cyberspace, as well as UN-based norms processes, according to Tom Burt, Corporate Vice President, Customer Security & Trust at Microsoft.[574] Although ostensibly neutral, the CyberPeace Institute is well-embedded within Microsoft's broad portfolio and vision of norms-oriented policy endeavours (and spin-offs).

5.1.4 Role Profiles: Pursuing Diplomatic Tracks

With reference to the activities outlined above, Microsoft has executed different roles in global cybersecurity norm formation processes. Apart from having acted as norm leader and cooperation incubator, it has orchestrated norms-related diplomatic efforts (diplomatic change agent), and has filled procedural as well as content-related gaps (gap

---

[573] Working Towards a Safer Online World for All (n 33).

[574] Tom Burt, CyberPeace Institute Fills a Critical Need for Cyberattack Victims (2019) ⟨https://perma.cc/3Y6C-RTQX⟩ accessed 6 March 2020.

filler). In the face of waning levels of trust in digital infrastructures and technologies, Microsoft has carried out these functions with a view to securing operational capacity, rebuilding confidence in digital products and services, as well as creating higher degrees of predictability in cyberspace. Vis-à-vis the tech giant's cooperation incubator role, Expert #3 has noted that

> there is lots of things that have influenced [Microsoft's] very active efforts in the area of cybernorms. If you look at just 2017, ... there was election tampering in the US that used email that involved Microsoft. Then we had WannaCry and NotPetya that also involved Microsoft. At the same time, there was the failed UN GGE report that was not published. Also, there were announcements of over 30 countries having offensive cybercapabilities. And when you put this all together, it gives the impression that states ... are having very big challenges they simply cannot meet and they cannot meet alone in any case. So, with [Microsoft's] rise of responsibility in this area, and the difficulties encountered by states, ... there has to be a more concerted partnership and effort by industry or civil society, of course, to be very active in this area.[575]

Other observers, including Daniel Dobrygowski, Head of Governance and Policy for the World Economic Forum Centre for Cybersecurity, too, have remarked moves by technology companies, including Microsoft, to form

> cybersecurity alliances and pacts with one another. These alliances are a symptom of the breakdown of trust between policymakers and those they [are] making polices for. Hundreds of companies – some of them, such as Airbus, Cisco, HP, Microsoft, Siemens, and Telefónica, among the largest in the world – have tried to step into this trust gap by forming groups around goals related to the future of the internet and digital networks. Some of these groups (... operational alliances) are mainly practical, sharing intelligence or technical data. Others (... normative alliances) are explicitly aimed at changing the ways companies deal with cybersecurity vulnerabilities and renegotiating the social contract between states and their citizens.[576]

Microsoft has launched cooperation-inspiring initiatives directed at various stakeholder groups, i.e. industry partners, civil society organisations, as well as governments, and

---

[575] Interview #3 (n 533).

[576] Daniel Dobrygowski, Why Companies Are Forming Cybersecurity Alliances (2019) ⟨https://perma.cc/2NN9-XZ5G⟩ accessed 14 September 2019, 2.

has released corresponding sets of norms and principles for these communities (please refer to the relevant initiatives, including the Cybersecurity Tech Accord as well as the Paris Call for Trust and Security in Cyberspace, and the Digital Peace Now campaign outlined earlier). In terms of numbers of initiatives launched as well as publicity generated, Microsoft has been a leader in the realm of promoting norms of responsible behaviour in cyberspace. Global technology services providers such as Cisco or Capgemini have underscored the tech giant's collaboration-enhancing function (e.g. vis-à-vis the Cybersecurity Tech Accord), and have mentioned Microsoft's leadership role.[577]

In concurrence with its cooperation incubator function, Microsoft has also acted as diplomatic change agent. Diplomatic change agents are entities seeking political engagement with a view to altering organisational setups and processes or political outcomes, and implementing new structures. Among other things, these actors assist in working out specific negotiations, cultivating relationships between different stakeholder groups, and ensuring 'the best possible treatment for their home' institutions.[578] With resources exceeding those of small nation states and targeted execution strategies, Microsoft has gained access to and made appearances at high ranking policy meetings. The company's Chief Legal Officer and President, Brad Smith, has played an instrumental role in Microsoft's foreign-policy-like endeavours. Brad Smith has acted as a cybersecurity envoy, of sorts, frequently attending international events alongside, or as expert discussant with political leaders and other high-ranking bureaucrats.[579]

According to a Time feature by Romesh Ratnesar,

---

[577] Steve Wanklin, Chief Cybersecurity Officer of the Capgemini Group, for instance noted 'Capgemini wholeheartedly embraces the idea of trying to reduce the impact of cybercrime on our society, but no organisation can defy the ever-evolving cybersecurity threats on its own. Therefore, we are very pleased to join the Cybersecurity Tech Accord and contribute to advancing its mission by collaborating on initiatives that improve the security, stability, and resilience of cyberspace', see Capgemini, Capgemini Joins Cybersecurity Tech Accord (2018) ⟨https://perma.cc/DT4V-LAEW⟩ accessed 28 August 2020.

[578] Farlex, Diplomatic Agents (2020) ⟨https://perma.cc/J57P-MZGE⟩ accessed 28 August 2020.

[579] Robert Gorwa and Anton Peez, Big Tech Hits the Diplomatic Circuit (2019) ⟨https://perma.cc/BQ82-MWBP⟩ accessed 28 August 2020.

> Smith, since becoming Microsoft's President, has focused as much on external relations as on internal strategy. With public distrust at its peak over the size, power and business practices of the tech industry's biggest companies, Smith has assumed the role of unofficial global ambassador for the industry. In [2018], he ... spent more than 100 days on the road, visiting 22 countries and pushing for collaboration between governments and tech companies to limit the destabilising effects of digital technologies.[580]

Among other things, he has been instrumental in crafting Microsoft's proposal for a Digital Geneva Convention as well as garnering industry-wide support for the Paris Call for Trust and Security in Cyberspace. According to Expert #3, Microsoft was

> very, very actively involved [(in the drafting and dissemination of the Paris Call principles)]. I would say that Microsoft was the main driver behind the industry and civil society involvement in the Paris Call. We have been engaged with governments as well, but considering the French had government-to-government cooperation, it was a joint effort. I mean, the French are the pen holders and that is clear. But we see it as building a community that could support a multistakeholder approach to cybernorms.[581]

Smith's rhetoric as well as the symbolism accompanying his activities (please refer to Figure 5.1 and Figure 5.2) have been inherently political. Microsoft's allusion to the Geneva Conventions of 1949, its linguistic references to constructs such as accord, or the company's picks of venues to present its normative proposals, including inside the Peace Palace in the Hague, represent deliberate and well-constructed rhetorical and figurative choices, signposting underlying diplomatic/political aspirations.

Further to its diplomatic change agent role, Microsoft has contributed to filling procedural and substantial (normative) voids. The company's gap filler role has been particularly evident in the wake of the non-consensus outcome of the 2017 UN GGE. With a view to maintaining momentum and bridging procedural voids, Microsoft has

---

580 Romesh Ratnesar, Microsoft's Brad Smith Wants to Restore Trust in Big Tech (2019) ⟨https://perma.cc/JYB5-S6W4⟩ accessed 16 September 2019.

581 Interview #3 (n 533).

Figure 5.1: Smith (second from right) taking part in meetings at the Élysée Palace with fellow business executives and statesman. The picture was taken in the remit of the 2018 Tech for Good summit hosted by French President Emmanuel Macron, see Romesh Ratnesar, Microsoft's Brad Smith Wants to Restore Trust in Big Tech (2019) ⟨https://perma.cc/JYB5-S6W4⟩ accessed 16 September 2019.

actively initiated/fed discussions on various fronts vis-à-vis different stakeholder groups (please refer to section *Activities: Engaging Extensively*) and has sought engagement with high-ranking officials. On the side-lines of the 2018 Munich Security Conference, for instance, it convened a workshop with 20 senior government officials and civil society representatives on gaps in international legal frameworks as they pertain to cyberspace. What, according to Paul Nicholas, Senior Director for Microsoft's Trustworthy Computing, emerged was 'a significant consensus on both the need to restructure cybersecurity discussions globally and the necessity of implementing the 2015 UN GGE report'.[582] As per Nicholas, the interactions also showed that 'the most significant challenge was seen as being structural: the lack of an international

[582] Paul Nicholas, Filling the Gaps in International Law Is Essential to Making Cyberspace a Safer Place (2018) ⟨https://perma.cc/MS7P-2FLL⟩ accessed 28 August 2020.

Figure 5.2: Smith (left) inside the Peace Palace in the Hague, introducing Microsoft's norms-oriented efforts to senior political leaders and academics, see The Hague Program for Cyber Norms, Dennis Broeders in Q&A and Discussion with Microsoft Global President and Chief Legal Counsel Brad Smith (2018) ⟨https://perma.cc/7C8J-78RV⟩ accessed 29 August 2020.

organisation or other venue for addressing the cyberthreat landscape of today and tomorrow'.[583] Following the discussions at the Munich Security Conference, Microsoft responded to the perceived structural mismatch outlined above with the launch of the Geneva-based CyberPeace Institute in September 2019. As stated on the organisation's website, the CyberPeace Institute 'intervenes where existing digital security systems are deficient', underscoring the intended gap-filling qualities of its founders.[584]

583 Filling the Gaps in International Law Is Essential to Making Cyberspace a Safer Place (n 582).

584 Working Towards a Safer Online World for All (n 33).

5.1.5 Effectiveness Review: Moving the Needle

In keeping with the introductory remarks, this section appraises Microsoft's normative contributions to debates about responsible behaviour in cyberspace along the three effectiveness dimensions of (a) output, (b) outcome, and (c) impact, and assigns corresponding contribution scores of (a) low, (b) medium, or (c) high to the company's undertakings.[585]

Output

Apropos output, the norms-based cyberinsecurity reduction measures undertaken by Microsoft have been remarkably successful. Since the non-consensus outcome of the 2017 UN GGE (and even leading up to 2017), Microsoft has produced respectable numbers of policy proposals, reports, blog posts, meeting records, as well as formal structures, and has supplemented these with targeted PR measures. Both in terms of substantive provisions as well as institutional commitments, the technology giant has provided relevant conceptual and practical inputs for furthering global peace and security in the virtual realm. The firm's interactions with industry fellows, non-governmental stakeholders, and governments have allowed it to promulgate strategically-relevant normative ideas. It has legitimised its normative advances in functional (functions executed), epistemic (knowledge brokered), and performance-related (scale and capabilities available) terms, and has usefully leveraged its market position and access to senior policy and technology circles to access and address relevant fora.[586]

Over the course of only a few years, Microsoft has created a far-reaching, multi-pronged, and organisationally well-integrated digital peace programme, which in terms of scope and profile has not been met by any other leading technology company to

---

585 For a recapitulation of the different evaluation benchmarks, please consult Table 3.3 in *Chapter 3*.

586 Anne Peters, Till Förster, and Lucy Koechlin, *Towards Non-State Actors as Effective, Legitimate, and Accountable Standard Setters* (Anne Peters and others eds, Cambridge University Press 2009) ⟨https://perma.cc/44ZV-ACEA⟩.

date. Furthermore, the activities undertaken by Microsoft have been noteworthy vis-à-vis sustaining momentum around discussions about rules of the road for the digital domain, and in drawing attention to the roles and ideational tenders of other non-governmental stakeholders, including the Global Commission on the Stability of Cyberspace, which has received funding from Microsoft for cybersecurity norms-related activities. With regard to the contribution scores mentioned above, Microsoft has demonstrated high levels of output effectiveness.

Outcome

Microsoft has pursued its cybersecurity norms-oriented activities with clear intentions to induce behavioural changes in state and non-state circles. Its principled advances vis-à-vis fellow industry partners (Cybersecurity Tech Accord), larger civil society (Digital Peace Now campaign), governments (Digital Geneva Convention), and mixed communities (Paris Call for Trust and Security in Cyberspace) have generated normative commitments from diverse stakeholders. As part of the Cybersecurity Tech Accord, for instance, signatories have collectively acted on their normative pledges by means of organisationally supporting cybersecurity capacity building initiatives, as well as endorsing and commenting on cybersecurity norms-related policy-making efforts of other entities.[587] Given the Cybersecurity Tech Accord's breadth of membership, instances of free-riding cannot be excluded unequivocally. However, they should not distract from the collective's broader achievements in relation to normative upshots. At the very least, the efforts undertaken by the Cybersecurity Tech Accord have further sensitised signatories to cybersecurity norms-related issues, including, for instance responsible vulnerabilities disclosure processes. Vis-à-vis the latter, in 2019, the Cybersecurity Tech

[587] For a list of policy submissions, please refer to Cybersecurity Tech Accord, Policy Submissions (2020) ⟨https://perma.cc/Y7QE-TMPH⟩ accessed 28 August 2020.

Accord committed to having all members adopt relevant disclosure policies, and has begun tracking progress publicly, and has established a collection of good practices.[588]

More generally, Microsoft has been exceptionally effective at being invited to and servicing high-ranking international cybersecurity policy venues with concrete proposals and ideational contents. Brad Smith, has been instrumental in advancing Microsoft's normative endeavours and leveraging his long-standing personal and policy connections to help the company gain access to pertinent venues. According to Fairbank, through engaging in discussions about responsible behaviour in cyberspace with governments and other prominent entities, Microsoft has increased its 'moral legitimacy and positive public image, building trust in its brand'.[589]

Journalists and scholars alike have taken note of the broad and influential range of normative efforts pursued by the tech giant. Matsakis, for instance, has noted that the tech giant's close collaboration with governments, such as the French Republic, evidences 'how tech corporations are playing a more active role in governing the internet. ... On the internet, corporations like Microsoft are increasingly taking on responsibilities once reserved for nation states'.[590] Through launching and co-sponsoring international policy initiatives such as the Paris Call for Trust and Security in Cyberspace, Microsoft has managed to secure political capital and has exerted influence beyond its traditional, technology-dominated confines. Moreover, through engaging politically (and normatively) Microsoft has effectively indicated that '[s]uccess in advancing cybersecurity requires an approach that is not only multinational, but

---

588 Cybersecurity Tech Accord, Leading by Example: Cybersecurity Tech Accord Welcomes New Signatories and Agrees to Implement Vulnerability Disclosure Policies across the Group (2019) ⟨https://perma.cc/CQJ4-PQDG⟩ accessed 28 August 2020; Cybersecurity Tech Accord, Vulnerability Disclosure Policies (2020) ⟨https://perma.cc/W8H9-DPC2⟩ accessed 28 August 2020.

589 Nancy Ayer Fairbank, 'The State of Microsoft?: The Role of Corporations in International Norm Creation' (2019) 4(3) Journal of Cyber Policy 380 ⟨https://perma.cc/GBZ2-ZAUJ⟩, 390.

590 The US Sits Out an International Cybersecurity Agreement (n 563).

multistakeholder in nature. This is because cyberspace, unlike the traditional planes of warfare like land, sea and air, is typically privately owned'.[591] Microsoft's presence at high-ranking cybersecurity norms meetings, as well as the ideational support received from different communities speak to its well implemented roles as diplomatic change agent and norm leader, and evidence the value of its political currency.

Impact

In contrast to other non-state entities such as the Global Commission on the Stability of Cyberspace or the Hague Programme for Cyber Norms, Microsoft, as a product- and services-oriented technology company, has found itself at an advantage vis-à-vis the the potential to yield direct impact. Sitting at the heart of cyberdefence-relevant control levers, Microsoft has from a technical point of view helped make the virtual realm more secure, e.g. by offering product updates and patches, analysing large amounts of threat data, as well as developing increasingly more resilient products. The norms-based activities outlined above have usefully supplemented Microsoft's technical cybersecurity activities. Its efforts to promote rules of the road for cyberspace have sought to contribute to a de-politicisation of norm formation processes, and a re-framing of cybersecurity norm-making ventures as collective undertakings of 'equals or colleagues steering outcomes towards a set of common goals'.[592]

From a business perspective, Microsoft's norms-oriented efforts have helped ameliorate the tech giant's public image and perception. According to survey results published by American technology news website the Verge in 2020, Microsoft has become viewed more favourably and more trusted among Americans compared to 2016. 75% of survey respondents stated that they trust Microsoft with their data, which is 6% more than the 69% who trust Google, and 34% more than the 41% of respondents who trust

[591] An Important Step Toward Peace and Security in the Digital World (n 561); Fairbank (n 589).

[592] Big Tech Hits the Diplomatic Circuit (n 579).

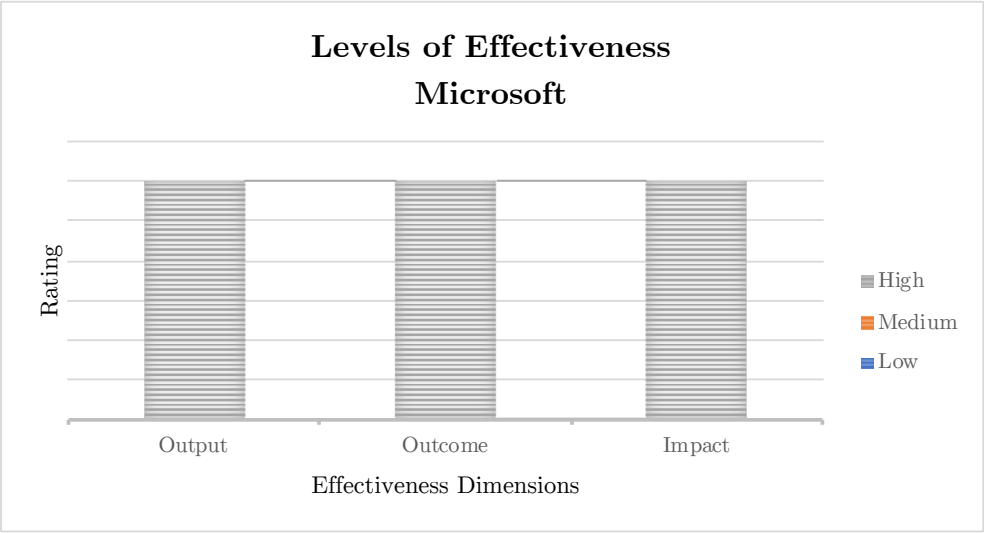

Figure 5.3: Effectiveness Plot: Microsoft.

Facebook with handling their information.[593] Although it is hard to establish direct and indisputable casual relationships between Microsoft's activities in the remit of norms of responsible behaviour in cyberspace and increasing levels of consumer trust, the nature of its efforts as well as its dedicated focus on trust and security indicate that Microsoft's norms-based undertakings have indeed had positive effects on its brand image and larger related strategic goals.

In terms of impact rating, Microsoft's efforts have had noticeable effects on debates about and framings of rules of the road for the virtual realm. Not only has the corporation managed to position itself as a key player and trusted source of advice across relevant policy fora, it has also been successful at gaining the support of different stakeholder groups for its propositions, thereby further extending its socio-political capital and influence.

[593] Casey Newton, The Verge Tech Survey 2020 (2020) ⟨https://perma.cc/DJ95-56SL⟩ accessed 28 August 2020.

5.1.6 Précis

Surveying the norms-based activities of one of the world's largest technology companies, this section has reasoned that Microsoft has made important substantive and structural contributions to cybersecurity norm formation processes. As norm leader, discussion feeder, and diplomatic change agent, it has developed an extensive suite of ideational proposals and has succeeded at rallying considerable numbers of different stakeholders behind its proposals. Conceptually and strategically, Microsoft's President, Brad Smith, has been instrumental in advancing the company's various programme components.

	Output	**Outcome**	**Impact**
High	Microsoft has produced respectable numbers of policy proposals, reports, blog posts, meeting records, as well as formal structures, and has supplemented these with targeted PR measures. It has created a far-reaching, multi-pronged, and organisationally well-integrated digital peace programme.	Microsoft's norm creation efforts targeted at fellow industry partners (Cybersecurity Tech Accord), larger civil society (Digital Peace Now campaign), governments (Digital Geneva Convention), and mixed communities (Paris Call for Trust and Security in Cyberspace) have generated norms-related commitments from diverse stakeholders.	Microsoft's efforts have had noticeable effects on debates about and framings of rules of the road for the virtual realm, and have increased the company's socio-political capital and influence.
Medium	-	-	-
Low	-	-	-

Table 5.1: Effectiveness Review: Microsoft.

Through its strategically aligned, multi-pronged normative activities as well as its frequent appearances on international policy stages, Microsoft has effectively contributed to altered imageries of norm development processes, supporting claims of post-national constellations. When it comes to peace and stability in the virtual realm, Microsoft appears to be on equal footing (equal partners) with governments in terms of ideational

force levied. Even though Microsoft's initiatives may not be legally binding, 'they carry weight by ceding some responsibility from elected officials to company representatives', as Gorwa and Peez have aptly stated.[594]

Microsoft's endeavours in the remit of responsible behaviour in cyberspace have already had broader systemic effects on political processes and have helped the company polish its corporate image as a responsible citizen and increase levels of trust and confidence in its products and handling of data. While the tech giant's normative efforts have been conducive to its public relations as well as its corporate social responsibility efforts, decision makers (both public and private) 'should be mindful of portraying tech firms and states as equal partners, and transferring diplomatic metaphors to the public-private realm', and should examine pertinent questions of accountability and legitimacy, as this manuscript will do as part of *Chapter 7*.[595]

5.2 Siemens: Wrestling to Raise the Bar

With operations spanning more than 200 countries, and revenues exceeding EUR 86.8 billion for fiscal year 2019, Siemens has become a 'global powerhouse' in the areas of electrification, automation and digitalisation.[596] Headquartered in Munich, Germany, Siemens has grown into one of the leaders in infrastructure and industry solutions, energy-efficient technologies, power generation/transmission capabilities, as well as medical diagnostics. Operationally, Siemens is segmented into three operating companies, i.e. Digital Industries, Smart Infrastructure, and Gas and Power; three strategic companies, i.e. Mobility, Siemens Healthineers, and Siemens Gamesa Renewable Energy; and a Financial Services (SFS) arm.[597] The Digital Industries

[594] Big Tech Hits the Diplomatic Circuit (n 579).

[595] Ibid.

[596] Siemens, About Us (2020) ⟨https://perma.cc/3EPV-4TF3⟩ accessed 9 March 2020.

[597] Siemens, *Annual Report 2019* (techspace rep, 2019) ⟨https://perma.cc/GFU3-J558⟩.

segment supports customers in discrete and process manufacturing apropos digital transformation and automation. The Smart Infrastructure arm provides intelligent solutions for integrating energy systems and building technologies. The Gas and Power division, offers 'products, solutions and services for generating electricity, for producing and transporting oil and gas, as well as for downstream and oil and gas-related operations'.[598] Siemens' Mobility branch is concerned with connected transport solutions for rail and road. Its Healthineers segment caters to the demands of healthcare providers and offers a broad portfolio of digital healthcare products and services. The activities of Siemens Gamesa Renewable Energy centre around the provision of wind turbines. And Siemens' Financial Services segment provides business-to-business financing solutions across the globe.[599] The organisational subdivision is part of Siemens' *Vision 2020+*, which seeks to award greater entrepreneurial freedom to the relevant segments and further improve customer focus as a consequence.

5.2.1 Background: Finding Partners

As is evident from the remarks above, Siemens' business segments boast considerable levels of digital exposure. Hence, from a strategic perspective, Siemens has strong motivations for maintaining trust and security in cyberspace. According to Roland Busch, member of Siemens' Managing Board and the company's Chief Operating Officer and Chief Technology Officer, 'cybersecurity is a key ingredient for trust of [Siemens'] customers in all [its] businesses offering digitally connected products. It is also the basis for sustainable success and the foundation of a strong ecosystem'.[600]

In the wake of several large-scale cybersecurity incidents in 2017, including WannaCry and Petya/NotPetya, which targeted Siemens product, the German industrial

[598] Siemens, *Annual Report 2019* (n 597).

[599] About Us (n 596).

[600] Siemens, Charter of Trust Partners Decide on Further Measures for More Cybersecurity (2020) ⟨https://perma.cc/23N3-VNKC⟩ accessed 25 March 2020.

conglomerate, together with eight partner corporations issued a *Charter of Trust* for the digital domain at the side-lines of the 2018 Munich Security Conference.[601] The launch of the Charter of Trust was a push by leading global industry heavyweights to (re-)instil confidence in digital technologies and services. Since the Charter's inauguration in February 2018, the number of sponsors has grown from nine to seventeen Charter partners, and four associate members.

Table 9.3 in the *Appendix* provides an overview of the supporters (as at March 2020), their sector affiliations, and (where applicable) sponsorship of other norms-related initiatives.

As part of their pledges, Charter members have vouched to undertake 'every effort to protect the data and assets of both individuals and businesses, prevent damage to people, businesses, and infrastructures and build a reliable basis for trust in a connected and digital world'.[602] Following multistakeholder-based lines of reasoning, Charter members have argued that collaboration between and concerted efforts among public and private sectors are vital for keeping pace with fast-changing technological advances, ever-evolving threat landscapes, and new criminal elements.[603]

5.2.2 Mandate and Goals: Promoting Principles-Based Strategies

With the intention of increasing cybersecurity and enabling trusted interactions among civil society, governments, and business enterprises, Charter signatories have released ten principles, spanning from ownership of cyber- and IT security, responsibility throughout the digital supply chain, security by default, user-centricity, innovation and co-creation,

601 Charter of Trust: For a Secure Digital World (n 33).

602 Ibid 1.

603 Charter of Trust, *Seeing Cybersecurity as an Opportunity* (techspace rep, Charter of Trust 2020) ⟨https://perma.cc/H56C-DFTS⟩.

to education, certification for critical infrastructure and solutions, transparency and response, regulatory framework, and joint initiatives.[604] While the Charter of Trust shares some tenets with other initiatives, including the Paris Call for Trust and Security in Cyberspace, its contents are less abstract and more practice-oriented in nature. Its stipulations are skewed towards tenets of responsible product development and engineering practices.[605] For instance, the Charter of Trust calls on governments and companies to work towards appointing dedicated personnel in charge of IT and cybersecurity (ownership), establishing supply chain-related security standards for IoT devices (supply chain protection), as well as third party certification schemes for critical infrastructures (critical infrastructure certifications), adjusting and further developing cybersecurity practices (innovation), and promoting cybersecurity rules and standards (regulatory framework) in a collaborative, multistakeholder manner (joint initiatives).[606]

5.2.3 Activities: Tackling Implementation

As far as promotional activities and implementation of the principles stipulated are concerned, Charter of Trust signatories have pursued phased strategies. Since the unveiling of the Charter of Trust at the Munich Security Conference, sponsors have conducted several roadshows and roundtables across three different continents (America, Europe, and Asia), and have participated in high-level governance summits, including the Paris Peace Forum and the UN Internet Governance Forum, as well as the

604 Siemens, *Siemens Annual Report 2018* (techspace rep, 2018); Private-Sector Initiatives for Cyber Norms: A Summary (n 216); Joe Kaeser, Working together for more security in the digital world (2018) ⟨https://perma.cc/U7VN-W9HG⟩ accessed 3 August 2018.

605 Maarten Van Horenbeeck and others, *Cybersecurity Agreements* (techspace rep, Internet Governance Forum 2019) ⟨http://www.intgovforum.org/multilingual/filedepot_download/4904/1658⟩.

606 Private-Sector Initiatives for Cyber Norms: A Summary (n 216); Siemens, Charter of Trust on Cybersecurity (2019) ⟨https://perma.cc/P2M9-EE62⟩ accessed 1 March 2020.

preparatory meetings of the G7.[607] They have also sought to contribute to certification-related discussions in the remit of the European Union Cybersecurity Act and have conducted Charter of Trust collaboration weeks, i.e. week-long, content-generating working sessions in the run up to the Munich Security Conference.[608]

Rather than pursuing cover-all approaches, Charter members have so far focused their efforts on three principles, namely ownership of cyber- and IT security, responsibility throughout the digital supply chain, and education.

Apropos principle one (ownership), Siemens, as one of the initiators of the Charter, has decided to create a new cybersecurity unit and appoint a new Chief Cybersecurity Officer (CCSO) with direct reporting lines to the Managing Board of Siemens AG. Other Charter of Trust members have taken comparable actions and have shared notions of urgency surrounding cybersecurity-related issues. Thomas Kremer, member of the board of Deutsche Telekom, for instance, has argued that

> [w]e [(Deutsche Telekom)] have to earn people's trust in digitisation. For this we need at least Europe-wide binding security standards that address the entire value chain and make security levels of hardware and software transparent for consumers and companies. ... When it comes to demands for more cybersecurity, a lot will help a lot. The more strong partners you get, the better for cybersecurity.[609]

With regard to principle two (responsibility throughout the digital supply chain), Siemens together with its fellow Charter partners has defined 'a list of minimum security requirements for all players in the supply chain, and effective mechanisms that can support their implementation'.[610] The list of 17 requirements is divided into eight

---

607 Siemens, One Year Charter of Trust: Important Milestones for More Cybersecurity (2019) ⟨https://perma.cc/8CTL-NEQD⟩ accessed 16 September 2019.

608 European Union (n 492).

609 Deutsche Telekom, Teaming Up For More Cybersecurity (2018) ⟨https://perma.cc/ZU9W-EAGH⟩ accessed 28 August 2020.

610 One Year Charter of Trust: Important Milestones for More Cybersecurity (n 607).

categories, and comprises elements such as security- and privacy-cognisant design of products and services, implementation of security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443, as well as execution of 'regular security scanning, testing and remediation of products, services, and underlying infrastructure'.[611] Since February 2019, the list of minimum cybersecurity requirements has been made compulsory for all new Siemens suppliers, and has been added as a binding clause to all new contracts and general ordering conditions. According to a corresponding press release issued by Siemens,

> [t]hese requirements will apply primarily to suppliers of security-critical components such as software, processors and electronic components for certain types of control units. Existing suppliers who do not yet comply with the requirements are to implement them gradually.[612]

Employing logics of scale, Siemens believes that '[if] all [its] partner companies put their global weight behind these measures and implement them together with their suppliers, [it] can generate tremendous impact and make the digital world more secure'.[613] Siemens' efforts seek to address the absence of uniform regulations governing the security of next-generation IT products, and promote security by default maxims.[614]

Concerning principle six (education), Charter of Trust signatories have started to develop and promote cybersecurity trainings for small and medium-sized enterprises (SMEs) as well as educational facilities, in particular institutions of secondary education.[615] In addition to providing free of charge training materials, Charter of Trust

---

611 One Year Charter of Trust: Important Milestones for More Cybersecurity (n 607). The eight categories include data protection; security policies; incident response; site security; access, intervention, transfer, and separation; integrity and availability; support; and training. For an overview of all 17 cybersecurity requirements, please refer to ibid.

612 About Us (n 596).

613 Ibid.

614 Charter of Trust Partners Decide on Further Measures for More Cybersecurity (n 600).

615 Charter of Trust, *Seeing Cybersecurity as an Opportunity* (n 603); Charter of Trust Partners Decide on Further Measures for More Cybersecurity (n 600). To illustrate, Charter of Trust

sponsors have also partnered with other organisations seeking to enhance cybersecurity education and knowledge exchange, for instance with the Alliance for Cyber Security, an initiative supported by the German Federal Office for Information Security (BSI) and the Federal Association for Information Technology, Telecommunications and New Media (Bitkom). To address the challenges facing cybersecurity training and education, e.g. skills gaps and lacking cybersecurity awareness, signatories have put forward 13 recommendations on how to address the latter. The recommendations include a broad bouquet of fairly high-level proposals mixing organisational and systemic (education systems) stipulations, including offering firm-wide cybersecurity courses/trainings, implementing security-conscious curricula across product and services design functions (to foster security-by-design-oriented mindsets), promoting cybersecurity as a sui generis career path, aligning educational capacities and skills with industry-relevant demands, as well as ensuring basic levels of cyberhygiene and cybersecurity education along unified standards and certification schemes.[616]

5.2.4 Role Profiles: Fostering Industry Cooperation

In seeking to stabilise and secure its operational environment, Siemens has executed the role of norm leader and cooperation incubator. The Charter of Trust has served as a key vehicle for creating continent-spanning connections among leading industry proponents, and furthering cross-sectoral pledges for common standards of responsible behaviour in the virtual realm. In acceding to Siemens' cybersecurity efforts, some of the Charter's founding members have made reference to the Charter's collaboration-fostering nature. Martina Koederitz, General Manager of IBM's US Industrial Market in North America and Board Member of the Charter of Trust, for instance, has argued that

members have created a 'special cybersecurity simulation for schools to give students and teachers a clear and easily digestible overview of the challenges', see Charter of Trust Partners Decide on Further Measures for More Cybersecurity (n 600).

616 Charter of Trust on Cybersecurity (n 606).

> [s]igning the Charter of Trust was merely the start of a collaborative process to improve security. ... Digital transformation is only going to succeed if people can rely on the security of data and connected systems. We must not hold back on building trust through ground[-]breaking initiatives like the Charter of Trust.[617]

Ruediger Stroh, Executive Vice President of semiconductor manufacturer NXP, has acknowledged that

> [c]omplementary to [NXP's] efforts as a market leader in secure connectivity, strengthening collaboration with partners from industry, governments and society is essential in developing new means and technologies that will protect [NXP's] future information systems and networks.[618]

While collaboration-related endorsements have been frequent, Siemens has also had to record two exits from its cybersecurity alliance. Italian energy giant Enel as well as founding member Daimler both decided to leave the Charter in 2019 and 2020, respectively.[619] Nonetheless, Siemens has been one of the few corporations which has actively initiated industry-focused, and alliance-furthering norm formation processes – the other prominent example being Microsoft.[620] Speaking to Siemens' norms-based leadership qualities, Shinichi Yokohama, Chief Information Security Officer of Japanese technology services company NTT, who joined the Charter in 2020, has noted that NTT intends 'to join the *shapers* community rather than waiting for the industry to be shaped', and as a result, supports 'global cross-industry collaboration [schemes] such as the Charter of Trust'.[621]

---

617 Martian Koederitz, Strengthening the Charter of Trust for a Secure Digital World (2018) ⟨https://perma.cc/WC7E-FAJ9⟩ accessed 28 August 2020.

618 NXP, NXP and Partners Sign Joint Charter on Cybersecurity (2018) ⟨https://perma.cc/XRD5-VDAF⟩ accessed 28 August 2020.

619 Rüdiger Köhn, Daimler Verlässt Allianz Gegen Cyberattacken (2020) ⟨https://perma.cc/8DCD-WX27⟩ accessed 31 March 2020.

620 Ruhl and others (n 314).

621 NTT, NTT Signed 10 Principles of the Charter of Trust (CoT) (2020) ⟨https://perma.cc/3DCL-6MUT⟩ accessed 28 August 2020.

Besides having acted as industry-minded norm leader and cooperation incubator, Siemens has also played the part of implementation assistant and capacity builder. Siemens has sought to further the putting into practise of provisions contained in the Charter as well as relevant and related provisions included in the 2015 UN GGE Report, or the Paris Call for Trust and Security in Cyberspace.[622] Together with its fellow Charter members, Siemens has taken concrete actions in the areas of cybersecurity education and digital supply chain security, and has gone beyond providing merely technical assistance. A pertinent example of the implementation-focused actions taken by Siemens has been the inclusion of base-line cybersecurity requirements across all supplier contracts and ordering conditions, as well as the propagation of security-by-default product features.[623] Given the vast scope of third parties interacting with Siemens' products and services, the contractual mandating of baseline cybersecurity requirements presents an important and potentially far-reaching step towards achieving higher levels of cybersecurity across complex international supply chains.

5.2.5 Effectiveness Review: Signalling High Ambitions

This section assesses the normative undertakings carried out by Siemens along the dimensions of output, outcome, and impact, and assigns corresponding ratings of low, medium, or high to the relevant effectiveness categories.

---

622 See, for instance, UN GGE norm (i), which holds that 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions', see United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26) 8, or principle six of the Paris Call, which seeks to 'strengthen the security of digital processes, products and services, throughout their life cycle and supply chain', see Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace (n 562).

623 With regard to implementing product-related security-by-default measures, Siemens has, among other things, upgraded the security settings of its supervisory control and data acquisition and human-machine interface system SIMATIC WinCC, see Siemens, Security Settings in WinCC (2020) ⟨https://perma.cc/U8B4-TUX2⟩ accessed 28 August 2020.

Output

Akin to its corporate fellow Microsoft, Siemens has released several norms-related artefacts, including principles, blog posts, presentations, audio-visual materials, and has further hosted numerous events under the conceptual umbrella of the Charter of Trust. In contrast to Microsoft, however, its activities have been more focused and targeted on partners from industrial sectors and have been less extensive than Microsoft's. Despite leveraging leading policy venues such as G7 or the Munich Security Conference to promote its norms-based activities pertaining to cybersecurity, Siemens' reach in terms of partners and supporters has been fairly restrained, with European corporations leading the way in terms of numbers.

Nonetheless, among industry conglomerates, Siemens has produced important conceptual guidelines pertaining to responsible behaviour in the virtual realm, in particular with regard to issues of supply chain security. From substantive as well as procedural perspectives, Siemens has supplemented some of its proposals with specific work plans and has embedded relevant focus provisions in its operational realities and those of its partners (reaching even beyond Charter of Trust signatories). However, beyond the focus areas outlined above (ownership of cyber- and IT security, responsibility throughout the digital supply chain, and education), operational follow-through, in particular on the parts of other Charter signatories, has been somewhat mixed.

According to Köhn, some of the Charter members have struggled with meaningfully linking Charter provision to their business strategies. Furthermore, Enel's and Daimler's decisions to leave the Charter have substantiated arguments of growing skepticism vis-à-vis the alliance's import.[624] Since the Charter's start in early 2018, membership has just about doubled, despite alleged claims of persistent expressions of interest from potential new members. Negotiations and debates among existing signatories have been said to

[624] Daimler Verlässt Allianz Gegen Cyberattacken (n 619).

be arduous, thorny, and time consuming, stalling implementation efforts and uniform approaches.[625] Taking these considerations into account, Siemens' output effectiveness can be rated as medium. Operational follow-through as well as strategic embeddedness have not (yet) been achieved across the board, and principles-related implementation efforts have been advanced somewhat unevenly and selectively across the ten focus areas.

Outcome

Vis-à-vis outcome, Siemens has managed to attract attention from leading (mostly Europe-based) industry conglomerates as well as political venues (Munich Security Conference) who have come to share common perceptions around cybersecurity risks and the need to successfully address these across various sectors. In terms of effecting behavioural changes among Charter of Trust signatories, however, Siemens' efforts have shown only slow rates of progress. The Charter's loose organisational set up as well as its consensus-oriented (but timid) leadership have not been conducive to generating greater alignment and concord among members with regard to operationalising the ten principles agreed upon and finding shared trajectories concerning their implementation. On the contrary, as Köhn has argued, the absence of strong direction as well as governance frameworks have hindered more rapid progress.[626]

Expert #4 has confirmed similar concerns. Regarding levels of engagement with the Charter members, Expert #4 has noted that the types of interactions with the Charter depend on

> how [many] other tasks there are at hand, what you can commit time-wise – the more you can commit, of course, the more fruitful the cooperation with the Charter of Trust turns out. Meaning, [however], that if there are other pressing issues, not much will happen with the Charter.[627]

---

625 Daimler Verlässt Allianz Gegen Cyberattacken (n 619).

626 Ibid.

627 Expert #4, Interview #4 (2019).

Apropos Siemens' ambition to foster consistent global approaches and regulatory cybersecurity frameworks, comprehensive substantiations of success have been missing.[628] According to a June 2020 presentation issued by the Charter of Trust, members sought to harmonise regulatory frameworks by shaping the political debate worldwide through foresight and reason. Specifics on how to go about changing regulatory realities, however, were not detailed.[629] Furthermore, despite its ostensibly politically-motivated interactions with G7 representatives, in particular the French government, and other world leaders in the remit of the Munich Security Conference, the Charter of Trust has received very few endorsements from non-members.[630] A rare example of public commendation from an intergovernmental organisation has been issued by OECD's Secretary-General, Jose Angel Gurria, who noted that '[t]he Paris Peace Call and the Charter of Trust launched at Munich Security Conference two years ago are excellent new forms of stakeholders working together for more cybersecurity by joining forces'.[631] Indeed, rather than garnering support from fellow state and non-state actors, Charter signatories have backed other normative alliances, e.g. the Paris Call for Trust and Security in Cyberspace, with a view to establishing connections between complementary initiatives and presumably elevating the Charter's international standing.[632] Overall, Siemens' outcome effectiveness can hence be rated as medium.

---

628 Charter of Trust, Driving Security in An Insecure World (2020) ⟨https://perma.cc/2EC3-73HX⟩ accessed 28 August 2020.

629 The relevant presentation line item was marked with N/A (not applicable), see ibid 10.

630 As per Chris Padilla, Vice President, IBM Government and Regulatory Affairs, the Charter's G7-related engagement was intended to 'educate policymakers ... and build more awareness. Much of the cybersecurity imperative is not only about technology but about people and good governance', see IBM, Charter of Trust Roadshow Brings Top Leaders to DC to Discuss Cybersecurity (2018) ⟨https://perma.cc/HHS3-TPK9⟩ accessed 28 August 2020.

631 Driving Security in An Insecure World (n 628).

632 Siemens, The Charter of Trust Takes a Major Step Forward to Advance Cybersecurity (2019) ⟨https://perma.cc/MU7Q-G784⟩.

Impact

As the lead initiator of the Charter of Trust, Siemens has set off notable principles-based cybersecurity processes, which if pursued diligently over the coming years have the potential to scale positively and improve the stability and security of the digital realm overall. In particular Siemens' efforts around fortifying digital supply chains and promoting security by default constitute measures which could possibly have far-reaching consequences, given the extensive numbers of third parties who could be asked to observe and comply with the latter. As things stand, however, Siemens has not reached the majority of goals set out in the Charter of Trust and in terms of stimulating political and systemic alterations, has lagged behind other industry giants, such as Microsoft. Ambiguities concerning the operationalisation of the stipulations contained in the Charter appear to have persisted, even three years after the launch of the Charter. Enel's and Daimler's exodus have served as severe cases of evidence in this regard.[633] In order to secure further progress and avoid further dismembering, Siemens is well advised to continue pursuing phased approaches to implementation.

According to Siemens' Global Head of Government Affairs, Eva Schulz-Kamm, the Charter was intended as 'an agreement that asks all members to take it seriously'.[634] As the remarks above have shown, degrees of commitment have varied and levels of responsibility among the signatories seem to have been dependent on the presence or absence of competing business priorities.[635] With the Charter of Trust, Siemens wanted to 'raise the bar on cybersecurity', however, the relevant normative measures to do so have, so far, remained in their infancy.[636]

---

633 Daimler Verlässt Allianz Gegen Cyberattacken (n 619).

634 Rob Spiegel, Siemens Pushes Cybersecurity to the Highest Levels (2018) ⟨https://perma.cc/4TPX-6RQV⟩ accessed 28 August 2020.

635 Interview #4 (n 627).

636 Siemens Pushes Cybersecurity to the Highest Levels (n 634).

While not having produced sweeping systemic changes, according to Experts #4 and #21, the Charter has yielded sensitising contributions. As per Expert #21 a key performance indicator of the Charter's success is 'the management attention within the companies' the initiative has generated.[637]

> Starting from Joe Kaesar [(Siemens)], going further to Deutsche Telekom, and IBM, there is really high management attention, which is also a factor of success. Because you have to organise it [(the implementation of the Charter principles)] within your company and you have to organise it of course, also within the network. So you have to have results, you have to have success in order to keep that management attention high.[638]

Confirming the Charter's sensitising qualities, Expert #4 has argued that

> in my perception, ... it [(cybersecurity)] probably did not have CEO attention, which it does by now. So, it has also been not only external lobbying and awareness raising, but also internal, meaning that the strategic importance has been noted also by board members now.[639]

In terms of effecting systemic impact, Siemens has been partially effective in the sense that it has begun operationalising some of the Charter principles, which given the scales of Siemens' supply chains as well as those of its Charter partners, already have some, and may have even more far-reaching security implications in the future.

5.2.6 Précis

This section has introduced the principles-based cybersecurity activities pursued by one of the largest industrial manufacturing companies in Europe. Surveying Siemens' normative undertakings, it has been proposed that with regard to prompting rules of the road for cyberspace, Siemens has acted as industry-minded norm leader and has also played the part of implementation assistant and capacity builder.

---

637 Expert #21, Interview #21 (2019).

638 Ibid.

639 Interview #4 (n 627).

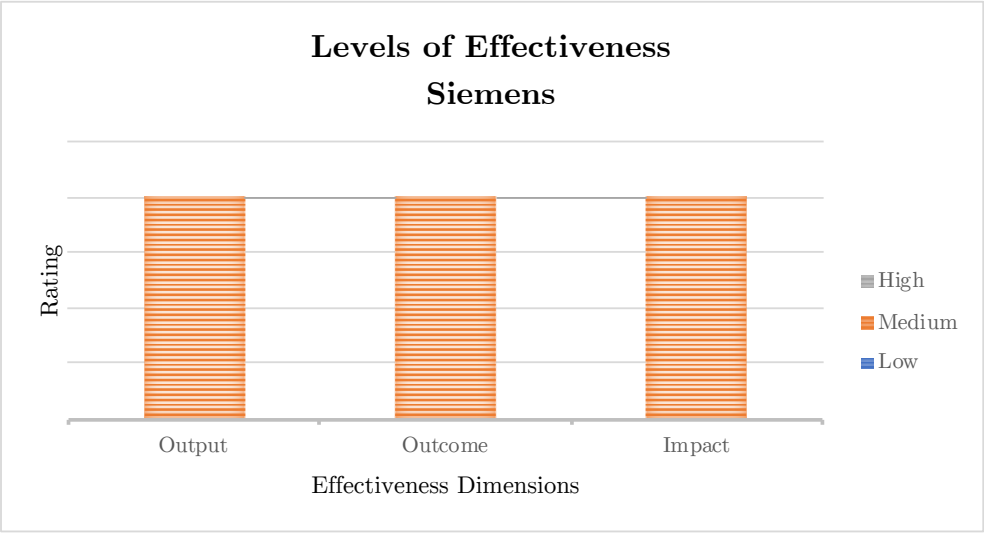

Figure 5.4: Effectiveness Plot: Siemens.

While multiple exodus from the Charter of Trust have cast doubts on the agreement's import and strength, and only a fraction of the Charter principles have seen preliminary implementation efforts, its activities have the potential to boast far-reaching security enhancements, given the extent of its third party networks as well as the contractually-driven (hands-on/practical) modalities of implementation pursued. In contrast to other technology heavyweights, in particular Microsoft, Siemens' political strategies and ambitions have not resulted in the same levels of public exposure and support. Its interactions with non-Charter members have been sporadic and narrow – shortcomings which have been recognised by the company's Global Head of Government Affairs, and are to be addressed in order to further advance the Charter and its contents.[640]

Future endeavours will tell if Siemens, together with its fellow Charter signatories, will manage to meaningfully 'raise the bar on cybersecurity' by pursuing principled approaches to cybersecurity.[641] As things stand, its efforts pertaining to furthering

[640] Daimler Verlässt Allianz Gegen Cyberattacken (n 619).

[641] Siemens Pushes Cybersecurity to the Highest Levels (n 634).

	Output	Outcome	Impact
High	-	-	-
Medium	Siemens has produced important conceptual guidelines pertaining to responsible behaviour in the virtual realm, in particular with regard to issues of supply chain security. From substantive as well as procedural perspectives, Siemens has supplemented some of its proposals with specific work plans and has embedded relevant focus provisions in its operational realities and those of its partners.	Siemens' efforts have shown only slow rates of progress in terms of effecting behavioural changes among signatories. The Charter's loose organisational structures have not been conducive to generating greater alignment and concord among members with regard to operationalising the ten principles agreed upon and finding shared trajectories on their implementation.	While not having produced sweeping systemic changes, Siemens has laid important cornerstones for operationalising some of the Charter principles, which may have far-reaching security implications in the future, e.g. binding supply chain security clauses.
Low	-	-	-

Table 5.2: Effectiveness Review: Siemens.

responsible behaviour in the virtual realm have not moved far beyond declaratory expressions of good intentions and preliminary considerations/building blocks of practical implementations. Moving from lowest common denominator approaches to genuine sector-crossing, norms-based cybersecurity activities is a lengthy task, which will require thorough assurances of commitment and demonstrations of problem-solving capabilities from all involved.[642]

5.3 Kaspersky Lab: Establishing New Benchmarks

Founded in 1997 by Eugene Kaspersky, Natalya Kaspersky, and Alexey de Mont de Rique, and headquartered in Moscow (Russia), Kaspersky Lab has become one of

[642] Daimler Verlässt Allianz Gegen Cyberattacken (n 619).

the largest privately-owned cybersecurity companies worldwide, with more than 30 subsidiaries. Since 1997 the company has gradually expanded its geographic footprint and revenues. The latter have grown to over USD 726 million.[643] Over the course of its existence, Kaspersky Lab has built up a customer base of more than 400 million private and over 270,000 corporate users.[644]

Antivirus, endpoint protection, and internet security products and services, which are offered to home users as well as small, medium, and large enterprises have long formed the core of Kaspersky Lab's business activities. As per information cited on its website, Kaspersky Lab has repeatedly been recognised as a leader in endpoint protection.[645] In 2019, Kaspersky Lab took part in 86 independent product tests and reviews, and outperformed competitors both in terms of numbers of tests entered into as well as ranks achieved.[646]

In addition to winning product reviews and customer satisfaction surveys, Kaspersky Lab's security expertise and threat intelligence activities have allowed it to uncover and contribute to analyses of malware attacks and cyberespionage efforts. In July 2017, for instance, Kaspersky Lab's Global Research and Analysis Team (GReAT) discovered a backdoor in a widely employed server management software product issued by NetSarang.[647] Labelled ShadowPad, the backdoor in NetSarang's software suite

---

643 Kaspersky Lab, Kaspersky Lab Announces 4% Revenue Growth to $726 million in 2018 (2019) ⟨https://perma.cc/9FJZ-ZHEQ⟩ accessed 17 August 2019.

644 Clement Guitton, *Inside the Enemy's Computer: Identifying Cyber Attackers* (Hurst & Company 2017); Kaspersky Lab Announces 4% Revenue Growth to $726 million in 2018 (n 643).

645 Kaspersky Lab Announces 4% Revenue Growth to $726 million in 2018 (n 643).

646 As part of the 2019 TOP3 evaluations of security vendors, Kaspersky Lab products were awarded 64 first and 70 top-three finishes, resulting in a TOP3 score of 81% Kaspersky Lab, TOP3 Scores (2019) ⟨https://perma.cc/ZQN8-NG9J⟩ accessed 31 March 2020. 'The TOP3 metric represents the aggregate scores achieved by over 80 well-known vendors in the security industry's most respected, independent tests and reviews', see ibid.

647 Kaspersky Lab, Kaspersky Lab's Global Research and Analysis Team Recognized for ShadowPad Discovery (2018) ⟨https://perma.cc/2ZND-HRMC⟩ accessed 31 March 2020. Among others, NetSarang's server management software products are used by large financial services providers, energy suppliers, as well as pharmaceutical companies, see Trend Micro, ShadowPad Backdoor

allowed intruders to collect relevant system information and, where applicable, deploy command and control capabilities. '[O]n command from the attackers, the backdoor platform would be able to download and execute further malicious code', exfiltrate data, or create processes.[648] When reporting the malicious activities, GReAT did not issue definitive statements of attribution but noted that 'certain techniques were known to be used in another malware like PlugX and Winnti, which were allegedly developed by Chinese-speaking actors'.[649] Upon discovery, Kaspersky Lab researchers immediately notified NetSarang, who promptly released a new and separate infrastructure, which according to news reports helped avert hundreds of system compromises.[650]

5.3.1 Background: Safeguarding Global Operations

In recent years, Kaspersky Lab has come under increasing scrutiny for alleged collaboration with the Russian government. The company's Russian origins as well as CEO Eugene Kaspersky's prior training by and engagement with Russian intelligence services (or closely affiliated entities) including the State Security Committee, KGB, have proven to be major stumbling blocks to Kaspersky Lab's operations, particularly in the US.[651] Following prior concerns, in September 2017, the US Department of Homeland Security ordered the removal of Kaspersky Lab products from all federal information systems (departments and agencies). According to a statement issued by then acting Secretary of Homeland Security Elaine Duke, the Department of Homeland Security was

Found in Server Management Software (2017) ⟨https://perma.cc/2Q5X-LPU6⟩ accessed 31 March 2020.

[648] Kaspersky Lab's Global Research and Analysis Team Recognized for ShadowPad Discovery (n 647); Charlie Osborne, ShadowPad: Backdoor in Enterprise Server Software Exposed (2017) ⟨https://perma.cc/9QTN-B4VK⟩ accessed 31 March 2020.

[649] Kaspersky Lab Global Research and Analysis Team, ShadowPad in Corporate Networks (2017) ⟨https://perma.cc/XTT8-RRNJ⟩ accessed 1 April 2020.

[650] ShadowPad in Corporate Networks (n 649); Dan Goodin, Powerful Backdoor Found in Software Used By >100 Banks and Energy Cos. (2017) ⟨https://perma.cc/2CFD-F7FN⟩ accessed 1 April 2020.

[651] Noah Shachtman, Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals (2012) ⟨https://perma.cc/P7YG-JFRL⟩ accessed 1 April 2020.

> concerned about the ties between certain Kaspersky [Lab] officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky [Lab] and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky [Lab], could capitalise on access provided by Kaspersky [Lab] products to compromise federal information and information systems directly implicates US national security.[652]

Kaspersky Lab vehemently denied any 'inappropriate' ties with its home government, arguing that no 'credible evidence' had been presented supporting the allegations made, and that the accusations were based on false assumptions as well as inaccurate interpretations of Russian regulations.[653] Furthermore, CEO Eugene Kaspersky argued that as a privately-owned company, Kaspersky Lab 'has no political ties to any government but [is] proud to collaborate with country authorities, international law enforcement agencies, and commercial and public entities in fighting cybercrime'.[654] In response to and with a view to mitigating the effects of claims of collusion with the Kremlin and fading levels of trust as well as operational bans, in late 2017, Kaspersky Lab decided to initiate a *Global Transparency Initiative*.

5.3.2 Mandate and Goals: Betting on Transparency

As per Kaspersky Lab's own attestation, the Global Transparency Initiative (GTI) represents

---

652 USDepartment of Homeland Security, DHS Statement on the Issuance of Binding Operational Directive 17-01 (2017) ⟨https://perma.cc/462A-ML4E⟩ accessed 1 April 2020.

653 Kaspersky Lab, Kaspersky Lab Response to Issuance of DHS Binding Operational Directive 17-01 (2017) ⟨https://perma.cc/YZJ8-WZRQ⟩ accessed 1 April 2020.

654 Kaspersky Lab, Our Principles of Cooperation with Law Enforcement Agencies, Commercial and Public Entities (2020) ⟨https://perma.cc/LF5Z-M73Z⟩ accessed 1 April 2020. Kaspersky Lab has been seen to collaborate with Interpol, the Federal Security Service of the Russian Federation and the Federal Service for Technical and Export Control of the Russian Federation, The City of London Police, The National High Tech Crime Unit of the Netherlands' Police Agency, Microsoft Digital Crimes Unit, as well as CERTs, among others, see ibid.

> a reaffirmation of the company's commitment to earning and maintaining the trust of its most important stakeholders: its customers. It includes a number of actionable and concrete measures to involve external independent cybersecurity experts and others in validating and verifying the trustworthiness of the company's products, its internal processes and business operations, and to introduce additional accountability mechanisms by which the company can further demonstrate that it addresses any security issues promptly and thoroughly.[655]

In terms of scope and depth, Kaspersky Lab's Global Transparency Initiative appears to stand out and differ from comparable benchmarks. Competitor McAfee, for instance, decided to shut down its source-code review programmes in 2017 out of fear of foreign interference and vulnerabilities identification/abuse.[656] Just as Siemens and Microsoft have used norms-based strategies in attempts to reassure and win (back) their customers' trust, so has Kaspersky Lab.[657] The Global Transparency Initiative has come to form an integral part of the company's mission to protect its customers from malicious cyberattacks around the globe, and has also come to serve as a useful tool for engaging with different sets of information security communities, both public and corporate. In contrast to the other two companies under investigation, Kaspersky Lab has been fairly straight-forward about the fact that the main purpose of the Global Transparency Initiative is to 'show the world that [the company] [has] nothing to hide', and that it can be trusted.[658] Rather than advocating for distinct sets of norms or action areas, however, Kaspersky Lab's norms-oriented activities have primarily revolved around three core principles, i.e. transparency (as the most obvious principle named), trust, and accountability, which have emerged in close relation to its operations and

---

655 Kaspersky Lab, Transparency Centres (2019) ⟨https://perma.cc/F826-R4TY⟩ accessed 18 August 2019.

656 Dustin Volz and Joel Schectman, McAfee Says It No longer Will Permit Government Source Code Reviews (2017) ⟨https://perma.cc/2ZDC-YLRZ⟩ accessed 18 August 2019.

657 Trust is one of the core components of the business models of all of the corporations surveyed as part of this chapter.

658 Kaspersky Lab, Kaspersky's Global Transparency Initiative Status Updates (2020) ⟨https://perma.cc/Q47K-HMUS⟩ accessed 2 April 2020.

issued third party business impediments, but at the same time appear to reflect larger industry trajectories.

5.3.3 Activities: Building New Structures and Broadening Access

In the remit of the Global Transparency Initiative, Kaspersky Lab has relocated its data processing and storage units from Russia to (neutral) Switzerland, and has begun to migrate European, American, and Canadian customer data.[659] In concurrence with the activities mentioned above, Kaspersky Lab has also established four Transparency Centres, which are located in Zurich (Switzerland), Madrid (Spain), Cyberjaya (Malaysia), and São Paulo (Brazil). The latter serve as dedicated sites for independent source code reviews, software updates, threat detection rules, and other technical and business processes by external parties, including regulators and government agencies responsible for cybersecurity, as well as enterprise partners of Kaspersky Lab.[660] Academics, media representatives, and other information security professionals have not yet been granted privileges to conduct assessments in the different Kaspersky Lab Transparency Centres, which raises questions as to Kaspersky Lab's sincerity vis-à-vis/committments to transparency and accountability.[661]

In addition to the Global Transparency Initiative, Kaspersky Lab has also participated in international security policy meetings, including at the United Nations. Among other things, Kaspersky Lab has used the Paris Peace Forum to advocate and garner support for its Global Transparency Initiative. As a backer of the Paris

659 The reasons cited by Kaspersky Lab for choosing Switzerland as the central data processing hub included (a) the country's 'long and famous history of neutrality', which according to Kaspersky Lab bears resemblance to the company's approach to malware detection and remediation, as well as (b) its stringent data protection rules, see Kaspersky Lab, Kaspersky Relocates Data Processing to Switzerland (2020) ⟨https://perma.cc/EF9V-N2BX⟩ accessed 5 April 2020.

660 Kaspersky's Global Transparency Initiative Status Updates (n 658).

661 Ibid.

Call for Trust and Security in Cyberspace, it has also made pledges to broader sets of cybersecurity principles, which go beyond engineering and data-processing practices. As a sef-proclaimed international advocate for transparency, Kaspersky Lab has further taken advantage of the opportunities provided to non-state actors in the context of the United Nations Open-ended Working Group (OEWG) to comment on proceedings and draft reports. In a position paper issued in March 2020, Kaspersky Lab noted that

> it continues to support the work of the OEWG [(which was sponsored by Russia in 2018]. This process, guided by inclusivity and transparency, and aimed at maintaining and increasing trust, has been an important step in keeping cyberspace secure, safe, open, and collaborative by engaging the entire global community, including private companies.[662]

With reference to the eleven norms issued by the 2015 UN GGE, Kaspersky Lab put forward suggestions for new norms focused on introducing/creating more transparency around the 'activities of Member States in cyberspace, particularly regarding offensive capabilities, and the rationale that informs such decision-making'.[663] Employing diplomatic tone and language, Kaspersky Lab specifically proposed the creation of additional norms relating to vulnerabilities disclosure processes, including the introduction of vulnerabilities equities processes, as well as coordinated vulnerabilities handling and mitigation processes.[664]

---

662 Kaspersky Lab, Comments on the Initial 'Pre-draft' of the Report of the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security (2020) ⟨https://perma.cc/8LLD-P9YB⟩ accessed 5 April 2020. See also Alex Grigsby, The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased (2018) ⟨https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased⟩ accessed 15 January 2019.

663 Comments on the Initial 'Pre-draft' of the Report of the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security (n 662).

664 Ibid.

5.3.4 Role Profiles: Raising Awareness on Multiple Fronts

In seeking to contribute to cybersecurity norm formation processes, Kaspersky Lab has acted as awareness raiser for its own causes as well as for wider issues concerning responsible behaviour in the virtual realm. The setting up of transparency centres across different continents has allowed Kaspersky Lab to disseminate its transparency-based security messages to diverse audiences, including governments, customers, as well as academics. The centres have made it possible for Kaspersky Lab to engage with and educate different communities re the trustworthiness of its products, internal processes, and business operations, as well as cybersecurity more generally. As noted in a report issued by UNIDIR in 2020, Kaspersky Lab has, among other things, helped spread knowledge about supply chain-related cybersecurity issues.[665]

> Although the scope and objectives of the Global Transparency Initiative do not exclusively focus on supply chain risk management (SCRM) or explicitly mention it, its framework serves as a de facto downstream supply chain assurance vehicle, allowing Kaspersky to demonstrate the absence of hidden functions in its products to its customers and regulators in national markets.[666]

In trying to improve levels of cybersecurity awareness, the Russian antivirus provider has also offered threat intelligence support to law enforcement agencies by way of providing threat intelligence reports, data feeds, as well as access to the company's Automated Security Awareness Platform, an online cybersecurity education tool.[667]

In the remit of the Paris Call for Trust and Security in Cyberspace, Kaspersky Lab has actively lobbied for trust-enhancing, cooperation-based policy measures, and has provided input to calls for contributions. For instance, in line with its image-reshaping

---

665 Oleg Demidov and Giacomo Persi Paoli, *Supply Chain Security in the Cyber Age* (techspace rep, United Nations Institute for Disarmament Research 2020) ⟨https://perma.cc/BFQ8-JW3X⟩.

666 Ibid 56.

667 Kaspersky Lab, *Supporting the Fight Against Cybercrime* (techspace rep, 2019) ⟨https://perma.cc/9BD4-R7QU⟩.

activities, Kaspersky Lab has proposed a 'shift to a paradigm of *verifiable trust*, the basis of which are to be found in digital trust and digital ethics'.[668] Moreover, CEO Eugene Kaspersky has acted as keynote speaker at the Paris Peace Forum, advocating for more trust and confidence in digital technologies, and showcasing the efforts undertaken by Kaspersky Lab in these regards.[669] In listing the reasons for Kaspersky Lab's attendance and support, the company's CEO noted that the Paris Peace Forum is an important

> annual event where folks from governments, business and other organisations come together to discuss and try and come up with ways to make the world better. And one of the hottest topics there, of course, was cybersecurity – and that's why [we] were extended a very enthusiastic invite. And since we support all kinds of initiatives throughout the world advocating international cooperation so as to create a digital world that is secure against all cyber-badness, we sent our RSVP back practically tout de suite.[670]

While corporate image-related concerns appear to have been key drivers behind Kaspersky Lab's norms-oriented activities, the ancillary cybersecurity awareness-enhancing qualities relating to/resulting from the company's efforts should not be disregarded.[671]

Closely linked to its awareness raiser role, Kaspersky Lab has also acted as implementation assistant and capacity builder. Cybersecurity capacity builders work towards empowering individuals, communities and governments to protect and further enhance the security and stability of their digital infrastructures. They typically help develop capabilities and competencies in the use of ICTs by providing assistance,

---

668 Anastasiya Kazakova, Enhance Trust in Cyberspace Through the Paris Call (2019) ⟨https://perma.cc/26QH-LQ7Y⟩ accessed 28 August 2020; Anastasiya Kazakova and Arnaud Dechoux, Working Together to Ensure Trust in and the Security of Cyberspace: Our Contribution to the Paris Call Consultation (2020) ⟨https://perma.cc/5LZS-45YU⟩ accessed 28 August 2020.

669 Sebastien Bequerel, Kaspersky au Paris Peace Forum (2019) ⟨https://perma.cc/5TV5-LG2Z⟩ accessed 28 August 2020.

670 Eugene Kaspersky, Bonjour, Monsieur President! (2019) ⟨https://perma.cc/WD5A-G9XB⟩ accessed 28 August 2020.

671 Demidov and Paoli (n 665).

promoting institutional reforms or organisational adaptations, and offering trainings to diverse stakeholders.[672]

As per Expert #22, and contrary to companies such as Siemens or Microsoft who have advanced specific sets of cybersecurity norms, for Kaspersky Lab

> it is not about developing norms ... it is rather about, firstly deliver some actual help, helping actual victims. And also increasing capabilities and ... supporting capabilities of those countries, underdeveloped countries, who just cannot afford purchasing [Kaspersky Lab's] reports, or who cannot afford developing their own instruments.[673]

Against this background, Kaspersky Lab has launched a *Cyber Capacity Building Program* as part of its Global Transparency Initiative, which aspires to support public and private entities in building relevant skills for identifying and mitigating security risks and conducting relevant security assessments. According to a white paper issued by the Russian antivirus provider, its programme is intended to help companies, government organisations, and academia in

> [b]uilding capacity ... to identify, evaluate and estimate risks related to external applications in their ICT infrastructure; [m]anaging identified risks and conducting an assessment of external applications for their integrity and security; [f]orming a list of requirements for external applications to minimise cybersecurity risks related to them; [and][d]eveloping an understanding of industry best practices for building a secure ICT ecosystem with regard to external applications.[674]

The capacity building modules developed by Kaspersky Lab include free 60-150 minutes long online training components on product security, thread modelling as well as code

---

672 Patryk Pawlak, *Riding the Digital Wave* (techspace rep, European Union Institute for Security Studies 2014) vol 21 ⟨https://perma.cc/FLP4-KTM4⟩; Zine Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace' (2019) 33(2) Global Society 224; Lilly Pijnenburg Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities* (techspace rep, Norwegian Institute of International Affairs 2015) ⟨https://perma.cc/KNY9-DXU8⟩.

673 Expert #22, Interview #22 (2019).

674 Kaspersky Lab, *Cyber Capacity Building Program* (techspace rep, 2020) ⟨https://perma.cc/5LZA-RNCP⟩.

review, and vulnerabilities management.[675]

Kaspersky Lab has supported both its awareness raising as well as its capacity building efforts with regular publications and blog posts on current cybersecurity issues drafted by (senior) members of staff. To illustrate, in the remit of its Global Transparency Initiative and in particular in the context of its Cyber Capacity Building Program, Kaspersky Lab has postulated five principles for responsible vulnerabilities disclosure practices, which revolve around building trust, informing relevant affected parties as a first priority, coordinating efforts, maintaining confidentiality, and incentivising white hat activates (i.e. vulnerabilities disclosures). In pursuance of disseminating these principles and positioning itself as a trailblazer (disposing of relevant capacities and know-how), Kaspersky Lab's Chief Technology Officer has contended that

> [f]or such an approach to work across the entire IT industry, however, other vendors – and their users, independent researchers, regulators, and other interested parties – must also use similar motives as their guides. Therefore, we decided to publish our principles for responsible disclosure of vulnerabilities found in other companies' software.[676]

5.3.5 Effectiveness Review: Remedying Public Perceptions

Consistent with the approaches pursued across the preceding case descriptions, this section evaluates the effectiveness of Kaspersky Lab's normative cyberinsecurity reduction efforts. The antivirus company's efforts are ranked as either high, medium, or low across the three effectiveness levers.

Output

Seeking to address negative public perceptions vis-à-vis its operations and products, Kaspersky Lab has released a diverse collection of trust-oriented instruments attempting

---

675 Kaspersky Lab, *Cyber Capacity Building Program* (n 674).

676 Andrey Efremov, Ethical Principles for Disclosing Vulnerabilities (2020) ⟨https://perma.cc/3NHY-STM2⟩ accessed 28 August 2020.

to thwart criticisms and mend its blemished image. Following the announcement of its Global Transparency Initiative in late 2017, Kaspersky Lab has taken concrete measures to support its thrusts for more security in the virtual realm. Apart from erecting brick and mortar structures across three continents, it has substantiated its structural commitments with strategically embedded policy engagements across leading cybersecurity norms venues, including the UN General Assembly First Committee processes as well as the Paris Peace Forum.[677] With a view to further anchoring its political undertakings, Kaspersky Lab has pursued collaborative engagements with law enforcement agencies, including Interpol, has participated at side events of heads of states meetings, e.g. the G77's *Workshop on Preventing and Combating Cybercrime supported by the Russian Federation and the United Nations Office on Drugs and Crime*, and has secured neutral assessments concerning its operations from political bodies such as the European Commission.[678] Kaspersky Lab has had to push hard for endorsements of its trust-oriented activities, and has only partially succeeded at attracting charitable appraisals pertaining to its operations (in contrast to Microsoft's endeavours in the remit of the Paris Call for Trust and Security in Cyberspace, for instance).[679]

In the context of its Global Transparency Initiative, it has created tactical associations with historically neutral and trusted entities, including, Switzerland, and has

---

677 Working Together to Ensure Trust in and the Security of Cyberspace: Our Contribution to the Paris Call Consultation (n 668).

678 Interview #22 (n 673); United Nations Office on Drugs and Crime, *Group of 77 Workshop on Preventing and Combating Cybercrime supported by the Russian Federation and the United Nations Office on Drugs and Crime* (techspace rep, United Nations Office on Drugs and Crime 2018) ⟨https://perma.cc/JUF5-BFG5⟩. In response to an inquiry brought forward by Member of the European Parliament, Gerolf Annemans, concerning allegations related to the security of Kaspersky Lab's products, the Commission stated that it 'is not in possession of any evidence regarding potential issues related to the use of Kaspersky Lab products', see European Commission, Answer Given by Ms Gabriel on Behalf of the European Commission (2019) ⟨https://perma.cc/C679-GVL2⟩ accessed 29 August 2020.

679 Oscar Williams, Exclusive: Kaspersky's Global Transparency Initiative Fails to Convince UK Government (2018) ⟨https://perma.cc/JW5K-ML22⟩ accessed 29 August 2020.

sought independent verification of its processes.[680] Rationalising the company's decision to relocate its customer data storage and processing as well as software assembly facilities, Eugene Kaspersky, has noted that

> [i]n a rapidly changing industry such as ours we have to adapt to the evolving needs of our clients, stakeholders and partners. Transparency is one such need, and that is why we [have] decided to redesign our infrastructure and move our data processing facilities to Switzerland.[681]

Apropos output effectiveness, the antivirus expert's norms-oriented undertakings have been firmly embedded in its corporate strategy and have been supplemented by numerous policy activities. Given the close connection between Kaspersky Lab's primary goal of ameliorating its public image and the advantages of normative strategies to do so, the high levels of output effectiveness do not astound.

Outcome

According to Expert #22 and in line with the effectiveness-related operationalisation proposals put forward by this thesis, endorsements from third parties are key markers of outcome effectiveness. As per Expert #22 Kaspersky Lab has received assurances from the European Commission, the French National Cybersecurity Agency (ANSSI), as well as the German Federal Office for Information Security (BSI). On the word of Expert #22, 'these were the most objective signs of support'.[682] While these assurances serve as important effect-related proxy indicators, evaluations pertaining to behavioural shifts of third parties as a result of Kaspersky Lab's norms-oriented undertakings are difficult to make, given the high degrees of secrecy surrounding the antivirus company's

680 Kaspersky Lab, Latest News on the Global Transparency Initiative (2019) ⟨https://perma.cc/F826-R4TY⟩ accessed 18 August 2019; Interview #22 (n 673).

681 Kaspersky Lab, Kaspersky Lab Moving Core Infrastructure from Russia to Switzerland; Opening First Transparency Center (2018) ⟨https://perma.cc/7T4L-VUUK⟩ accessed 29 August 2020.

682 Interview #22 (n 673).

customer base, and limited public data available pertaining to the frequenting of its transparency centres/interactions with regulators.[683]

Apart from having won assurances of some national supervisory authorities and regional organisations, Kaspersky Lab has taken advantage of submitting proposals to UN General Assembly First Committee norm construction processes and being present at global peace events, including the Paris Peace Forum. The world's third largest vendor of consumer IT security software has effectively used these high-profile policy platforms for tendering its ideas and creating images of trustworthiness and accountability, thereby furthering both its business and ideational goals. Through committing financial and human resources, and putting in place new organisational structures supporting its norms-oriented endeavours, Kaspersky Lab has elevated benchmarks for other vendors of security products and introduced norms-inspired competitive differentiators, which have the potential to affect the strategic priorities of its competitors.

Although primarily driven by economic and public relations concerns, Kaspersky Lab has assumed responsibilities which stretch beyond its core business interests. The technology company has made sizeable investments to advance policy issues around verifiable trust and digital ethics, which may at times even be at odds with its immediate economic concerns (e.g. with regard to the protection of intellectual assets). Overall, Kaspersky Lab's transparency-oriented undertakings have yielded fair results across the output dimension.

Impact

As a global provider of information security software solutions, Kaspersky Lab's activities have had direct links to matters of cyberresilience and -stability. Through its

683 Empirical data and regular reports relating to Kaspersky Lab's Global Transparency Initiative, e.g. numbers of visits, types of requests received, etc. have been scarce.

bug bounty programmes, threat intelligence efforts, and antivirus products for home users, small and medium sized enterprises, and large corporations, Kaspersky Lab has contributed to options for maintaining adequate levels of stability in the virtual realm.

In terms of goal attainment, its transparency-based activities have supported the company in partially recovering from the espionage allegations levied against it in 2017. They have also assisted the antivirus provider in laying the groundwork for the advancement of changed expectations among public and private entities vis-à-vis standards of corporate transparency in the context of cybersecurity. In light of Kaspersky Lab's dominant underlying risk management motivations, however, it is questionable, to what extent 'frameworks for establishing appropriateness' and advancing digital ethics have responded to and affected larger, systemic issues of trust and accountability in cyberspace. While having won neutral assurances from political entities such as the European Union, other political bodies, e.g. the UK government, have been more guarded in their evaluations of Kaspersky Lab's efforts and have somewhat tainted the success of the company's transparency-related undertakings.

According to an article issued by the New Statesman in late 2018, discussions between Kaspersky Lab and Westminster around the Global Transparency Initiative did not contribute to alleviating Westminster's concerns around potential reconnaissance and data exfiltration activities conducted on behalf of the Russian government. According to the same source, a senior government security spokesperson held that

> [w]e [(the UK government)] are grateful to Kaspersky [Lab] for working with us and being transparent. We are aware of [the new Swiss data centre] opening and we see it as a really good step in the right direction. At the moment, that step is not far enough for us to change our advice [(i.e. to refrain from employing Kaspersky Lab solutions across UK government and critical national systems)].[684]

[684] Exclusive: Kaspersky's Global Transparency Initiative Fails to Convince UK Government (n 679); Ian Levy, Managing Supply Chain Risk in Cloud-Enabled Products (2017) ⟨https://perma.cc/SN2G-4NM9⟩ accessed 29 August 2020.

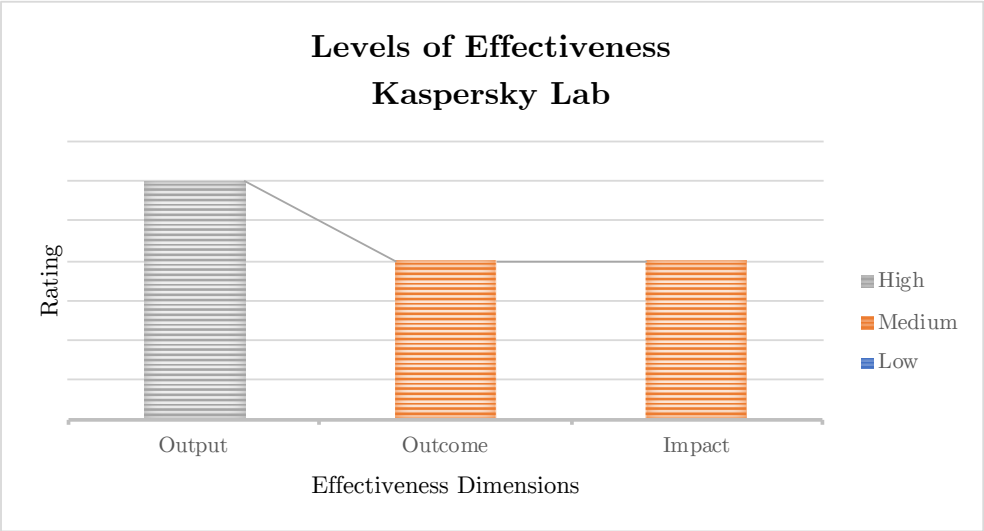

Figure 5.5: Effectiveness Plot: Kaspersky Lab.

Hence, in relation to earning (back) and maintaining the trust of its customers – previous, existing, and future – Kaspersky Lab has only partially succeeded. From systemic as well as operational considerations, Kaspersky Lab's norms-oriented undertakings have not extensively redefined cybersecurity-related interactions among offensive and defensive actors in cyberspace nor led to wider fundamental changes in how peace and stability are provided and perceived.

5.3.6 Précis

Grounded in attempts to dispel allegedly false accusations around the employment and workings of its products and services, Kaspersky Lab has resorted to transparency-based strategies to ameliorate public perceptions around its operations as well as to secure business-related capacities. In close alignment with its overarching corporate strategy, this chapter has argued that in the remit of promoting norms of responsible behaviour in cyberspace, Kaspersky Lab has executed the roles of awareness raiser and capacity builder. Kaspersky Lab has created higher levels of awareness for both

its own circumstances as well as for wider issues including accountability and trust in cyberspace. In the context of its Global Transparency Initiative, Kaspersky Lab has built up structural as well as human resources to assist other entities in improving their risk exposures and verifying Kaspersky Lab's processes, thereby elevating industry standards and competitive positioning. According to a former company spokesperson, '[t]rust and transparency are a challenge for the whole industry and with [the Global Transparency Initiative], Kaspersky Lab is setting the benchmark'.[685] Furthermore, seeking greater political coverage, the antivirus company has issued contributions to and pursued engagements with governments or government-near entities, including, for instance, Interpol or the Paris Call communities, and has strategically placed its ideas and proposals across high-ranking policy fora.

Kaspersky Lab has been quite overt and pragmatic about the use of norms-inspired instruments to change the views around its operations. The company's former Vice President of Public Affairs, for instance, has noted that '[t]he allegations we [(Kaspersky Lab)] faced are wrong and there is no evidence. Still the allegations are there. We need to show customers we are taking them seriously and address them'.[686] Even though business interests may have been the primary motivators behind its transparency-based initiatives, Kaspersky Lab has gone beyond issuing high-level, public relations-inspired commitments, and has started to provide yardsticks for transparency-guided interactions in the virtual realm.[687] In terms of output, Kaspersky Lab's efforts have been very effective, and vis-à-vis outcome and impact have yielded fair results. Whether these efforts will have long-term effects on the perceived levels of cybersecurity and 'be enough to assuage growing fears of digital espionage, however, remains to be seen'.[688]

---

685 Exclusive: Kaspersky's Global Transparency Initiative Fails to Convince UK Government (n 679).

686 Rachel England, Kaspersky to Move to Switzerland Following Latest Government Ban (2018) ⟨https://perma.cc/UA3C-SWKU⟩ accessed 29 August 2020.

687 Interview #22 (n 673).

688 Kaspersky to Move to Switzerland Following Latest Government Ban (n 686).

	Output	Outcome	Impact
High	Kaspersky Lab has taken concrete measures to support its thrusts for more security in cyberspace. Apart from erecting brick and mortar structures, it has substantiated its structural commitments with strategically embedded policy engagements across leading cybersecurity norms venues.	-	-
Medium	-	Kaspersky Lab has elevated benchmarks for other vendors of security products and introduced norms-inspired competitive differentiators, which have the potential to affect the strategic priorities of its competitors.	Kaspersky Lab has contributed to options for maintaining adequate levels of stability in the virtual realm. Alterations in cybersecurity-related interactions among offensive and defensive actors or wider fundamental changes in how peace and stability are provided have not taken hold.
Low	-	-	-

Table 5.3: Effectiveness Review: Kaspersky Lab.

5.4 Stakeholder-Cluster Synthesis: Shaping Strategic Environments

This chapter has scrutinised and evaluated the effectiveness of the norm formation activities pursued by three major technology firms, *Microsoft*, *Siemens*, and *Kaspersky Lab*. Although situated in different business areas and offering different products and services, all of the companies surveyed have boasted high levels of exposure to threats emanating from cyberspace. As a consequence and with a view to securing

their operations and products, these industry representatives have become increasingly active in debates about rules of the road for the digital domain. Indeed, as has been evidenced by this chapter, technology companies have come to exert considerable discursive and jurisgenerative power over discussions about responsible behaviour in cyberspace, and their (public) postures have come to resemble those of global diplomatic actors. According to Wheatley, non-state protagonists with jurisgenerative capacities are private actors, capable of establishing

> international governance norms that frame the context for action by states, corporate entities and individuals. To the extent that their jurisgenerative efforts have practical effect, non-state actors exercise political authority, an activity traditionally associated with the state.[689]

Thematic analyses of primary and secondary materials pertaining to the three corporate actors studied have underscored their jurisgenerative capacities. Examinations have revealed that in the remit of creating rules of the road for the virtual realm, the corporate non-state actors analysed have taken on multiple different roles. They have stimulated cooperation among like-minded stakeholders (cooperation incubators), have championed norms (norm leaders), and filled procedural as well as content-related gaps (gap fillers). Moreover, they have increased awareness concerning their activities and have acted as capacity builders/implementation assistants. In contrast to the strong sensitising qualities exerted by civil society and academic actors, the contributions of the technology firms surveyed have primarily been of substantive and procedural natures in the sense that they have contributed to the substantive underpinnings of cybersecurity norms (specified existing norms or introduced new norms), and have broadened participatory baselines.

As part of their endeavours, the three corporate case study actors have generated impressive numbers of candidate norms for increasing the stability and security

689 Wheatley (n 168) 220.

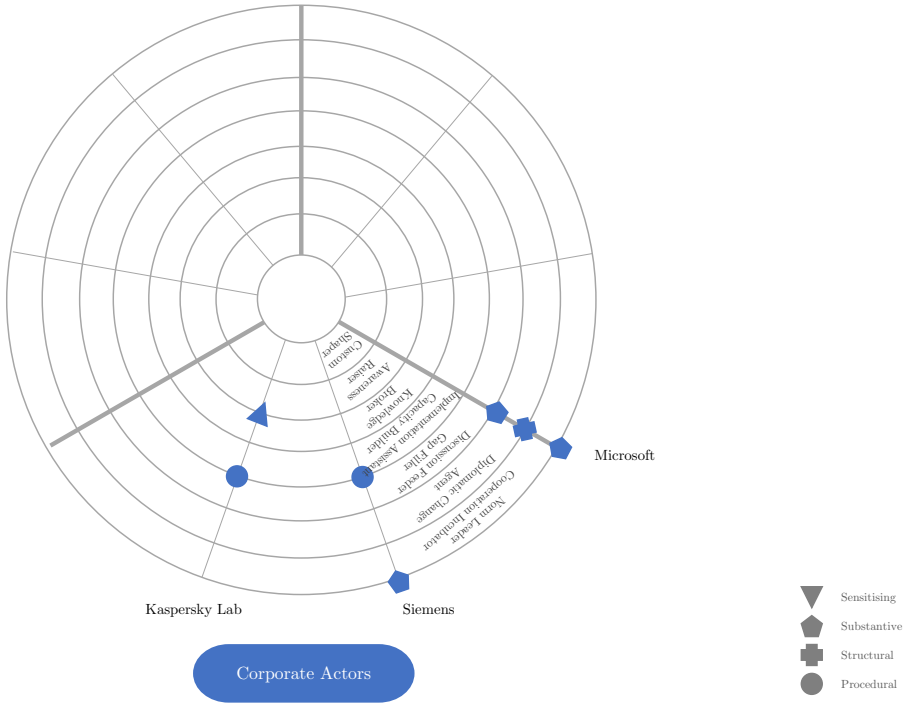

Figure 5.6: Corporate Actors Contributions Spectrum.

of the digital realm. Furthermore, they have been successful at signalling their political intentions and promoting/injecting their normative proposals across high-ranking diplomatic venues, including the United Nations, the G7 and the G20, as well as the European Union. In line with these observations, the three corporate actors surveyed have been attested medium to high levels of output and outcome effectiveness. Comments made by interview partners have substantiated the relevant effectiveness ratings.[690] For instance, in terms of engagement strategies pursued, Expert #11 has noted that

> ... it is an exciting time because we are finding and discovering platforms that are best suited to sort of facilitating input from the multi-stakeholder community, including in this case, private industry... . So whether that is participating in ... working groups that are government established, ... where we can sort of have some input and guidance on to what our best practices are, whether it is just vocally supporting and being very public

690 Interview #3 (n 533); Interview #4 (n 627); Interview #22 (n 673).

> about which types of proposals we think are wise and well informed ... . And then of course, we also write independent white papers that have to do with things like norm development, but then also other cyberspace policy issues that we think are important and valuable [and] implicit to this discussion as well. And then we also seek to find ways to sort of partner with others to amplify our voices. And so ... a great example of this would be the Cybersecurity Tech Accord.[691]

In contrast to the previous cluster of case studies analysed (civil society and academic actors), technology companies have also been seen to initiate tentative systemic changes. These corporations sit at the heart of ICT infrastructures and, among other things, have the option to implement normative proposals in technical terms rather than *just* political terms, i.e. in very practical terms. As has been noted by Cornish and Kavanagh, and has been revealed by the case study analyses, private sector entities, including the ones surveyed as part of this chapter, have 'been heavily engaged in promoting *productive behaviours*. ... In the increasingly urgent, practical matter of ensuring the security, functionality and stability of cyberspace', private sector entities have become essential parts.[692] And their public postures in debates about rules of the road in cyberspace have come to reflect these realities as well as their critical degrees of importance.

---

[691] Expert #11, Interview #11 (2019).

[692] Cornish and Kavanagh (n 356) 14.

Multistakeholder approaches that include representatives from civil society organisations, business, technology, and academia might help to increase awareness about norms for [cyberstability] at different levels of governance, which also raises the likelihood of their being adopted and adhered to.

— Alexander Klimburg & Virgilio Almeida, *Cyber Peace and Cyber Stability: Taking the Norm Road to Stability (2019)*

6 Expert Communities

Contents

This chapter presents the third cluster of case studies under investigation. Following analyses pertaining to the governance inputs of civil society, academia, and corporate actors, this chapter explores the roles assumed by expert communities. Expert communities are collectives of professionals or specialists with extensive knowledge and expertise across specific issue areas. Examples of such groups include commissions, think tanks, as well as professional networks and confederations. Expert communities are typically bound together by shared principled beliefs, practices, and goals, often relating to specific political or economic problems.

This chapter surveys three instances of expert communities. Specifically, it analyses

the cybersecurity norm creation activities of (a) the *Global Commission on the Stability of Cyberspace (GCSC)*, (b) the *Forum of Incident Response and Security Teams (FIRST)*, and (c) *Carnegie Endowment for International Peace*. In terms of structure, this chapter adheres to the organisation of the previous case studies, and begins with short contextual remarks concerning the actors under review, goes on to examine their activities, and then identifies their role profiles, before assessing the effectiveness of their undertakings.

The presence of and increasing influence exerted by independent experts on questions relating to public ordering has been widely acknowledged. Indeed, recourses to independent stocks of knowledge and expertise have not been rare occurrences in the fields of international law and international relations. Among other things, public organs have been seen to employ specialists to conduct independent reviews, issue policy advice, legitimise courses of action taken by decision makers, and accomplish concrete policy goals.[693] Inputs by and turns to expert communities have not gone unchallenged, however. Questions such as '[h]ow, and by whom, are these experts selected, [w]hat criteria are employed for their appointment, [h]ow is their independence ascertained and maintained' have at times remained elusive or been answered controversially.[694] Keeping these questions in mind, this chapter examines the norm creation activities undertaken by the Global Commission on the Stability of Cyberspace before evaluating the undertakings by FIRST and Carnegie Endowment for International Peace.

---

693 Valentina Carraro, 'Electing the Experts: Expertise and Independence in the UN Human Rights Treaty Bodies' (2019) 25(3) European Journal of International Relations 826 ⟨https://perma.cc/8DS3-68YV⟩; James G McGann, *Think Tanks, Foreign Policy and the Emerging Powers* (James G McGann ed, Springer International Publishing 2019) ⟨https://perma.cc/Z9UL-U4S4⟩; Christina Boswell, 'The Political Functions of Expert Knowledge: Knowledge and Legitimation in European Union Immigration Policy' (2008) 15(4) Journal of European Public Policy 471 ⟨https://perma.cc/338R-JB48⟩; Peter M Haas, 'Introduction: Epistemic Communities and International Policy Coordination' (1992) 46(1) International Organization 1 ⟨https://perma.cc/M5AD-ZRVT⟩.

694 Carraro (n 693) 827.

6.1 Global Commission on the Stability of Cyberspace: Moulding Peaceful Interactions

Launched by the Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (following invitations by the Government of The Netherlands), the Global Commission on the Stability of Cyberspace (hereinafter referred to as *GCSC* or the *Commission*) was set up with the intention of contributing to international peace and security agendas related to cyberspace over the course of three years, 2017-2019.[695] The unveiling of the GCSC followed the conclusion of earlier multistakeholder-oriented expert processes, including the *Global Conference on CyberSpace (London Process)* and the *Global Commission on Internet Governance (GCIG)*. The Global Commission on Internet Governance was introduced at the World Economic Forum in January 2014 by the Centre for International Governance Innovation and Chatham House, and brought together twenty-nine experts from different geographies and backgrounds, including from policy, government, academia, and civil society.[696] Postulating that 'internet governance is one of the most pressing global public policy issues of our time', the so-called Bildt Commission was convened with a view to offering guidance on how to address emerging challenges concerning the digital domain, and ensuring multistakeholder-based governance models.[697] Following two and a half years of deliberations and meetings,

695 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492).

696 Chatham House, Global Commission on Internet Governance (2019) ⟨https://perma.cc/F99V-44CN⟩ accessed 25 November 2019. As vehicles of consultation and examination, independent expert commissions have been employed across a wide variety of different policy contexts for many years. Prominent examples, include, for instance, the Brundtland Commission on sustainable development or the Palme Commission on disarmament and security issues. According to Evans, '[h]igh-level panels and commissions have become in recent decades a very busy second-track diplomatic industry. Since the 1980s, more than thirty commissions have come and gone, harnessing the collective talents of over five hundred individual commissioners and panellists to report on issues across the security, development, and general governance spectrum', see Gareth Evans, 'Commission Diplomacy' in Andrew F Cooper, Jorge Heine, and Ramesh Thakur (eds), *The Oxford Handbook of Modern Diplomacy* (Oxford University Press 2013) ⟨https://perma.cc/J9QE-CJHJ⟩ 1.

697 Global Commission on Internet Governance, *One Internet* (techspace rep, Centre for International Governance Innovation and Chatham House 2016) ⟨https://perma.cc/GL8F-FFMS⟩. Carl Bildt,

the GCIG's twenty-nine commissioners concluded their work with the adoption of the *One Internet* report in June 2016.[698] Targeted at policymakers, private industry participants, members of the technical community, and other stakeholders, the report stressed 'the need for a new social compact designed to protect the rights of users, establish norms for responsible public and private use, and ensure the kind of flexibility that encourages innovation and growth'.[699]

In contrast to intergovernmental expert commissions, the GCIG and the GCSC were led by leading global think tanks, rather than by governments or government-affiliated entities. Irrespective of their uncharacteristic founderships, however, the typical features of expert commissions as laid out by Evans in the context of expert gatherings at (state-based) multilateral venues also hold true for the GCIG and the GCSC, respectively. According to Evans,

> [t]he distinctive characteristics of these commissions and panels are that they are convened to address particular international policy problems (albeit often extremely broadly defined); the problems they address are global rather than country-specific or regional in scope; their advice, though formally sought by a particular international organisation, government, or combination of sponsors, is directed to the broader international community; their membership is international; they are independent in character, with their members appointed in their personal capacity rather than as representatives of their states or organisations, even if holding executive office at the time; and they have a finite rather than ongoing lifespan (most commonly two to three years).[700]

---

former Prime Minister and former Foreign Minister of Sweden, oversaw the activities of the GCIG.

698 Global Commission on Internet Governance (n 697).

699 Camino Kavanagh, 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (August, Washington, DC, 2019) ⟨https://perma.cc/9MCZ-NTQB⟩ 9.

700 Evans (n 696) 278.

6.1.1 Background: Assembling Expertise

Following preparatory meetings held by the HCSS and the EastWest Institute in August 2016, the Global Commission on the Stability of Cyberspace was officially inaugurated at the sidelines of the Munich Security Conference in February 2017.[701] With a view to creating a multistakeholder-based pool of experts, the HCSS and the EastWest Institute called together twenty eight regionally-diverse scholars, Chief Executive Officers (CEOs), and (former) policymakers to form the GCSC. Some of the commissioners appointed to the GCSC had already contributed to the work of the Bildt Commission.[702] Table 9.4 in the *Appendix* provides an overview of the individuals appointed to the GCSC, their other (previous/current) positions held, their country affiliations, as well as their records with the GCIG.

While the list of commissioners clearly exudes eminence and professional know-how, the composition statistics are heavily skewed towards Western-oriented mindsets, with only one Russian industry representative, one expert from South America, and two Chinese think tank envoys represented on the GCSC (see Table 6.1).[703] Furthermore, in terms of multistakeholder-orientation, the composition statistics reveal concentrations of former/current government delegates and experts affiliated with think tanks or academic research institutions (see Table 6.2).[704] Industry spokespersons are the least frequently represented stakeholder group on the GCSC (with a share of 11%), followed by representatives from civil society with a share of 18%.

---

[701] The Hague Centre for Strategic Studies, Launch of Global Commission on the Stability of Cyberspace (2017) ⟨https://perma.cc/VGQ3-XT8J⟩ accessed 26 November 2019. Parts of this chapter have been published as Eggenschwiler, 'Expert Commissions and Norms of Responsible Behaviour in Cyberspace: A Review of the Activities of the GCSC' (n 340).

[702] Please refer to Table 9.4 for more details.

[703] The division of commissioners by region follows a continent-based logic. Russia, for example, is included in the category *Europe*, whereas Israel, for instance, figures in the category *Asia*.

[704] Policy and academic research institutions are represented as single category entitled *Academia/Think Tank*.

Region	Count of Commissioners	Percentage
Africa	2	7.14%
Asia	8	28.57%
Europe	8	28.57%
North America	9	32.14%
South America	1	3.57%
Grand Total	28	100.00%

Table 6.1: Geographical Distribution of Commissioners.

Sector	Count of Commissioners	Percentage
Academia/Think Tank	11	39.29%
Civil Society	5	17.86%
Government	9	32.14%
Industry	3	10.71%
Grand Total	28	100.00%

Table 6.2: Sectoral Distribution of Commissioners.

Between February 2017 and March 2019, the GCSC was chaired by Marina Kaljurand, and later, following her election to the Estonian Parliament and subsequent withdrawal from the position as Chair of the GCSC, co-led by Michael Chertoff and Latha Reddy.

In conducting its activities, the GCSC has received operational and administrative support from (a) a dedicated secretariat, (b) a management board, composed of key financial contributors, including for instance the Ministries of Foreign Affairs of the Netherlands and France, the Cyber Security Agency of Singapore, Microsoft, Afilias, and the Internet Society (ISOC), (c) a government advisory board, made up of state representatives, as well as (d) a research advisory group led by four moderators.[705]

[705] Global Commission on the Stability of Cyberspace, Information Sheet (2018) ⟨https://perma.cc/3DEY-6MEP⟩ accessed 4 February 2019. In addition to the four organisational entities listed above, the GCSC has also received backing from four special advisers, including, Carl Bildt, Vint Cerf, Sorin Ducaru, and Martha Finnemore, as well as from the Federal Department of Foreign Affairs of Switzerland, GLOBSEC, the Ministry of Foreign Affairs of Estonia, the Ministry of

		Count	Percentage
Region	Africa	2	7.14%
	Asia	8	28.57%
	Europe	8	28.57%
	North America	9	32.14%
	South America	1	3.57%
	Grand Total	28	100.00%
Sector	Academia or Think Tank	11	39.29%
	Civil Society	5	17.86%
	Government	9	32.14%
	Industry	3	10.71%
	Grand Total	28	100.00%

Table 6.3: Combined Commissioner-Related Distributions.

6.1.2 Mandate and Goals: Enhancing International Security Through Multistakeholder Efforts

With the intention of 'develop[ing] proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace' in a multistakeholder-oriented fashion, the activities of the GCSC have revolved around three main deliverables, i.e. (a) facilitating information exchange, (b) supporting basic research, and (c) advocating proposals for action.[706] The GCSC has sought to achieve its goals by means of holding regular physical meetings, funding scientific analyses, and issuing publications, including *Commission Positions* and *White Papers*.[707]

Internal Affairs and Communications of Japan, the African Union Commission, Black Hat USA, DEF CON, the European Union Delegation to the UN in Geneva, the Global Forum on Cyber Expertise, Google, the Municipality of The Hague, Packet Clearing House, Tel Aviv University, and the United Nations Institute for Disarmament, see Global Commission on the Stability of Cyberspace, About (2020) ⟨https://perma.cc/2XFC-5JEJ⟩ accessed 8 January 2020.

[706] The mission statement, as phrased by the GCSC inception group gathered by the HCSS and the EastWest Institute, read: '[t]he Global Commission on the Stability of Cyberspace (GCSC) will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace. The GCSC will engage the full range of stakeholders to develop shared understandings, and its work will advance cyberstability by supporting research, information exchange, and capacity building', see Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492).

[707] Information Sheet (n 705).

6.1.3 Activities: Developing Global Norms

Since its inception in February 2017, the Commission has convened alongside or taken part in several high-ranking internet policy meetings, including the Munich Security Conference, CyCon, Black Hat and DEF CON, the Global Conference on CyberSpace, the International Cybersecurity Forum, GLOBSEC, CYBERSEC, the Singapore International Cyber Week, UNIDIR, OSCE, and G20 cybersecurity meetings, ICANN, EuroDIG, IETF, the Global Forum on Cyber Expertise, Israel's Cyber Week, the UN GGE regional consultations, the UN Open-ended Working Group intersessional consultative gatherings, the Paris Peace Forum, as well as the Internet Governance Forum.[708] In addition to debating orders of business and ensuring face-time among the commissioners, these meetings have served as strategic components in relation to the GCSC's goals to reach out and receive inputs from diverse stakeholder communities, and complete advocacy activities.

Building on initial feedbacks received and following nine months of on- and offline deliberations among the commissioners, the GCSC introduced its first norm, a *Call to Protect the Public Core of the Internet* on the margins of the Global Conference on CyberSpace in New Delhi in November 2017.[709] Six months later, in May 2018, it released its second norm, a *Call to Protect the Electoral Infrastructure*, following the conclusion of GLOBSEC 2018.[710] In November 2018, after another six months of opinion gathering events and meetings, the Commission published a norm package comprising another six rules of the road for cyberspace. The so-called *Norm Package Singapore* contained the following stipulations: (a) a norm to avoid tampering, (b) a

[708] Global Commission on the Stability of Cyberspace, News Archive (2019) ⟨https://perma.cc/BZ8V-JABA⟩ accessed 29 November 2019.

[709] Global Commission on the Stability of Cyberspace, *Call to Protect the Public Core of the Internet* (n 509).

[710] Global Commission on the Stability of Cyberspace, Call to Protect the Electoral Infrastructure (2018) ⟨https://perma.cc/TX6L-FDMH⟩.

norm against commandeering of ICT devices into botnets, (c) a norm for states to create a vulnerabilities equity process, (d) a norm to reduce and mitigate significant vulnerabilities, (e) a norm on basic cyberhygiene as foundational defense, as well as (f) a norm against offensive cyberoperations by non-state actors.[711]

Norms (a) and (b) of the Norm Package Singapore call on state and non-state actors not to 'tamper with products and services in development and production', and not to 'commandeer others' ICT resources for use as botnets', while norms (c) and (e) explicitly urge governments to enact 'appropriate measures, including laws and regulations, to ensure basic cyber[hygiene]', and to 'create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities'.[712] Norms (d) and (f) request non-state actors to 'prioritise security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities [and] take measures to timely mitigate vulnerabilities', and to refrain from 'engaging in offensive cyber[operations]' (hack-backs).[713]

The Norm Package Singapore 'is the result of contributions and extensive consultations by GCSC commissioners, advisory experts and the GCSC Research Advisory Group'.[714] As per information contained in the Norm Package Singapore, in sketching out the norms proposed, the Commission pursued *bottom-up* and *top-down* norm generation strategies, and was guided by

> significant shared core beliefs ... [, including] the importance of a democratic, multistakeholder approach to governance, the necessity to promote development and economic growth, the need to balance rights and responsibilities

---

711 Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (n 33).

712 Ibid 9-13; 16-17.

713 Ibid 12-13; 18-19.

714 Global Commission on the Stability of Cyberspace, Global Commission Introduces Six Critical Norms Towards Cyber Stability (2018) ⟨https://perma.cc/M43W-8L7R⟩ accessed 5 February 2019.

> for both states and individuals, and the centrality of cyberspace remaining open and unimpeded in its operations.[715]

During the public hearings held in the remit of the fourth full Commission meeting conducted in Singapore in September 2018, the GCSC received inputs from envoys from UNIDIR, the United Nations Office for Disarmament Affairs (UNODA), the UN Secretary-General's High-level Panel on Digital Cooperation, the OSCE and the European Union, as well as from government officials from the United States, the United Kingdom, Switzerland, Singapore, Poland, Norway, New Zealand, the Netherlands, Mexico, Kenya, Japan, India, Hungary, Germany, France, Finland, Estonia, Canada, Belgium, and Australia. A smaller number of civil society and private actors also took part in the public hearings, including the Asia-Pacific Network Information Centre (APNIC), FIRST, ICANN, Microsoft, JPMorgan Chase, and the S. Rajaratnam School of International Studies.[716]

The norms elaborated by the Commission were crafted with the express intention of contributing to an architecture of greater security and stability in cyberspace, and being adopted and implemented by public as well as private actors.[717] Apropos substance and scope, the norms advanced by the GCSC take into account and draw on different sources of inspiration, including the 2013 and 2015 UN GGE reports, contributions of leading private organisations, think tanks, as well as scholarly papers. As has been mentioned, the *Call to Protect the Public Core of the Internet*, for instance, was first articulated by Associate Professor of Security and Technology, Dennis Broeders, in a study published by the Netherlands Scientific Council for Government Policy.[718]

---

[715] Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (n 33) 6. These values essentially represent Western notions of cyberspace and cybersecurity.

[716] Global Commission on the Stability of Cyberspace, *GCSC Meeting Singapore: Attendance List* (techspace rep, 2018) ⟨https://perma.cc/G4VF-J8RJ⟩.

[717] Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (n 33).

[718] Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance*

In contrast to the eleven norms proposed as part of the 2015 UN GGE report, the eight norms put forward by the GCSC exhibit a more technical, operationalisation-oriented phrasing, which may be a by-product of having different stakeholders, including very technical participants, with different priorities at the table, and needing to achieve consensus. At the same time is to worth noting that the Commission purposely intended to 'amplify and expand' the normative provisions contained in previous agreements and 'point the way to new opportunities for increasing the stability of cyberspace'.[719]

In terms of aspirational evocation, norms such as ensuring adequate levelsh of cyberhygiene (norm (e)) or reducing and mitigating significant vulnerabilities (norm (f)) resemble fairly obvious standards in the context of increasing the stability and security of cyberspace, and appear to reflect politically fairly uncontentious, lowest common denominator outcomes. At the same time, these norms are likely to offer valuable quick wins (low-hanging fruits) with regard to securing implementation of at least some of the prescriptions issued by the GCSC.

In the run-up to the conclusion of its three-year mandate, the GCSC supplemented its eight norms with a *Cyberstability Framework*. Introduced as part of the Commission's final report, the Cyberstability Framework was devised with the intention of helping 'the international community in promoting the stability of cyberspace while taking into consideration the rapid, unprecedented pace of technological change that significantly and continuously alters cyberspace'.[720]

The framework as proposed by the Commission contains seven core components, including (a) multistakeholder engagement; (b) the formulation of principles; (c) the

(n 491). The study argued for the establishment of an international norm directed at protecting 'the internet's public core – its main protocols and infrastructure, which are a global public good – ... against unwarranted intervention by states', see Dennis Broeders, 'Aligning the International Protection of the Public Core of the Internet with State Sovereignty and National Security' (2017) 2(3) Journal of Cyber Policy 366 ⟨https://perma.cc/8X93-CMUR⟩, 367.

719 Global Commission on the Stability of Cyberspace, *Norm Package Singapore* (n 33) 7.

720 Global Commission on the Stability of Cyberspace, *Final Report Fact Sheet* (n 565) 1.

creation and implementation of voluntary norms; (d) adherence to international law; (e) the enactment of confidence and (f) capacity building measures; as well as (g) the promulgation of technical standards. As per its own attestation, the Commission primarily focused its efforts on enabling multistakeholder exchanges and creating principles and norms but recognises the need for more concerted efforts touching on all seven elements of the framework.[721]

With a view to providing input for further progress apropos rendering cyberspace secure and stable, the GCSC issued six high-level recommendations. Specifically, the GCSC suggested that:

> (a) State and non-state actors adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action.
>
> (b) State and non-state actors, consistent with their responsibilities and limitations, respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.
>
> (c) State and non-state actors, including international institutions, increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of different parties.
>
> (d) State and non-state actors collect, share, review, and publish information on norms violations and the impact of such activities.
>
> (e) State and non-state actors establish and support [c]ommunities of [i]nterest to help ensure the stability of cyberspace.
>
> (f) A standing multistakeholder engagement mechanism be established to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.[722]

The idea of forming *communities of interest*/communities of practice for operationalising normative commitments has also reverberated across other fora, including

---

[721] Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492). According to the Commission, adherence to the following principles is critical for ensuring the stability and security of cyberspace: (a) responsibility; (b) restraint; (c) requirement to act; and (d) respect for human rights, see ibid 18-19.

[722] Global Commission on the Stability of Cyberspace, *Final Report Fact Sheet* (n 565) 2.

the Paris Peace Forum and the Internet Governance Forum (notably across the Best Practice Forum on Cybersecurity).[723] Communities of interest denote groups of parties/stakeholders who harbour expertise and share concerns for pertinent policy issues/problems. They are learning systems that interacting on an ongoing basis with the goal to devise palpable solutions to fairly well-defined/narrow problem sets.[724]

6.1.4 Role Profiles: Filling Gaps and Fostering Cooperation

As is evident from the remarks above, in seeking to guide responsible behaviour in cyberspace and fulfilling its mandate, the GCSC has taken on different roles, some of which resemble more traditional non-state actor functions, and others of which represent more novel manifestations of non-state actor responsibilities. Thematic reviews of GCSC-related primary and secondary materials have revealed three principal role profiles (themes): (a) awareness raiser, (b) discussion feeder and gap filler, and (c) norm leader and cooperation incubator.

Awareness raiser represents one of the more traditional non-state actor roles taken on by the Commission.[725] The Commission has made it one of its key priorities to '[promote] mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity', and has been recognised for its advocacy efforts by other stakeholders, including the Cybersecurity

723 Best Practice Forum on Cybersecurity (n 384); Maarten Van Horenbeeck, The Operationalization of Norms and Principles on Cybersecurity (2019) ⟨https://perma.cc/42ZF-DR7J⟩ accessed 7 December 2019.

724 MITRE Corporation, Community of Interest and/or Community of Practice (2016) ⟨https://perma.cc/4LWR-HXYT⟩ accessed 8 January 2021.

725 Awareness raisers typically inform and educate public and private entities about salient policy issues with a view to bringing about changes in attitudes and behaviours, and generating improved outcomes, see Sayers (n 390); Abbott and Snidal, 'The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State' (n 42).

Tech Accord.[726] Members of the Cybersecurity Tech Accord have noted that the GCSC is an entity that

> has a critical role to play in raising awareness and understanding of issues related to international peace and stability, specifically in driving responsible state and non-state behaviour in cyberspace. It has embraced this mission with a spirit of collaboration with other key stakeholders and has been open to different perspectives and views.[727]

In terms of executing its awareness-raising efforts and delivering information and key messages to private and public target audiences, the Commission has benefited from work conducted by the Research Advisory Group as well as its diverse member base. The GCSC, through its representatives, has been able to secure access to a range of different communities and fora (otherwise hard to gain entry to), including technical, governmental, and academic gatherings, and has supported its meeting and outreach activities with steady feeds of publications and commentaries by individual commissioners.[728] Furthermore, it has kept interested parties abreast with monthly *Cyberstability Updates* and engagement opportunities.[729] Importantly, the Commission has executed its awareness-raising activities both through aggregate and individual

---

[726] Wolfgang Kleinwächter, *Towards a Holistic Approach for Internet Related Public Policy Making* (techspace rep, Global Commission on the Stability of Cyberspace 2018) ⟨https://perma.cc/9MJU-GDGC⟩ 4.

[727] Cybersecurity Tech Accord, The Cybersecurity Tech Accord Welcomes the Global Commission's Singapore Norm Package, Offers Comments on Enhancing Stability in Cyberspace (2019) ⟨https://perma.cc/ZC9T-5FFR⟩ accessed 30 September 2019.

[728] See, for instance, Wolfgang Kleinwächter, The Kaljurand Commission: Building Bridges Over Troubled Cyber-Water (2017) ⟨https://perma.cc/VC97-F5V8⟩ accessed 23 April 2018; Kleinwächter, *Towards a Holistic Approach for Internet Related Public Policy Making* (n 726); Joseph SJr Nye, A Normative Approach to Preventing Cyberwarfare (2017) ⟨https://perma.cc/D2E3-UDJL⟩ accessed 10 November 2017; Joseph SJr Nye, How Will New Cybersecurity Norms Develop? (2018) ⟨https://perma.cc/9NLG-HZJC⟩ accessed 31 May 2018; Joseph SJr Nye, Eight Norms for Stability in Cyberspace (2019) ⟨https://perma.cc/M2DP-SQ6M⟩ accessed 6 December 2019; Chris Painter, *Deterrence in Cyberspace* (techspace rep, Australian Strategic Policy Institute Limited 2018) ⟨https://perma.cc/H9XT-TBM9⟩; Motohiro Tsuchiya, A Difficult Road to International Norms for Cybersecurity (2019) ⟨https://perma.cc/6MF2-S3BJ⟩ accessed 8 December 2019.

[729] Global Commission on the Stability of Cyberspace, Monthly Update Archives (2019) ⟨https://perma.cc/VWK8-YUUY⟩ accessed 8 December 2019.

commissioner-led efforts, which has allowed it to increase its reach into different stakeholder groups (technical, governmental, academic).[730]

A less typical role taken on by the Commission is the role of *discussion feeder and gap filler*. This role was most prominently articulated as part of the expert interviews.[731] Expert #5, for instance, has argued that the Commission

> feed[s] the discussion ... with concrete proposals. ... [T]he self-understanding of the Commission is – that was also the reason for its establishment – [that] there is a need for certain norms in the field of cybersecurity. We have seen a discussion for fifteen years in the First Committee of the United Nations [General Assembly] which has produced some norms, ... and then you could see, in 2016/17, there will be no consensus to go the next step. And the risk was that this will lead to a bad situation, a standstill. So, ... this was the motivation for the establishment of the Global Commission, to say, while governments at this moment are unable to take the next step, and to move [forward] from the 2015 report, ... in the meantime, we as a multistakeholder group, ... do the work which should be done by governments, but we try to open their eyes and say ... you [governments] have to take on board also the opinions, perspectives, and ideas of non-state actors.[732]

Further corroborating these remarks, Expert #2 has held that

> the self-portrait of the Commission is that it tried to fill a vacuum, left by states being unable to effectively work together on this issue and then tried to respond to the increasing threat scenario, and ... [bring] together individuals from different stakeholder groups and [look] at norms that would apply to state and non-state actors. I think its self-portrait is really that it tried to fill these various gaps. ... I think there is a strong commitment in the Commission that international cooperation and multistakeholder cooperation is really important. And that at the time that we started our work, neither was – in the field of cyberstability and -security – really happening effectively.[733]

---

730 See Kurowska (n 184).

731 Expert #13, Interview #13 (2019); Expert #2, Interview #2 (2019); Expert #5, Interview #5 (2019), see also Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (n 16).

732 Interview #5 (n 731).

733 Interview #2 (n 731).

Secondary sources, too have taken note of the gap-filling activities undertaken by non-state actors. In his 2017 publication, Mačák, for instance, held that the 'voluntary retreat [of states] has left a power vacuum, enabling non-state actors to move into the space vacated by states and pursue various forms of *norm entrepreneurship*'.[734]

The third role taken on by the Commission is the role of *norm leader and cooperation incubator*. The GCSC has been widely recognised for its norm generation activities and has been commended for its multistakeholder-driven efforts towards developing rules of the road for cyberspace.[735] In terms of quality and scope, the Commission's ideational efforts and attempts at exercising regulatory clout in discussions pertaining to transnational cybersecurity governance have stretched beyond standard notions of norm entrepreneurship. The Commission has actively proposed cyberstability-related regime components and has, as a consequence, employed mobilisation strategies that differ from typical non-state actor norm entrepreneurs.[736] Rather than relying on naming and shaming, and antithetical persuasion strategies, for instance, the Commission has offered cooperation-oriented conceptual tools for making greater strides towards enacting rules of the road for the virtual realm.[737] The GCSC has acted at 'two consecutive stages of norm emergence in two different roles simultaneously': as norm (or moral) entrepreneur as well as as norm leader or regime proponent, respectively.[738]

Supporting these insights, Expert #9 has maintained that

> we [(the Commission)] do not want to be a norm factory. We want to produce norms but we also want to give a picture for the future. ... At the

---

734 Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (n 16) 10.

735 Ido Kilovaty, 'Privatized Cybersecurity Law' UC Irvine Law Review ⟨https://perma.cc/UBR6-SVZ8⟩; The Cybersecurity Tech Accord Welcomes the Global Commission's Singapore Norm Package, Offers Comments on Enhancing Stability in Cyberspace (n 727); Maarten Van Horenbeeck, FIRST Address to the Global Commission on the Stability of Cyberspace (2018) ⟨https://perma.cc/B8SD-GUUY⟩ accessed 27 November 2018.

736 Flohr and others, *The Role of Business in Global Governance* (n 219).

737 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492).

738 Flohr and others, *The Role of Business in Global Governance* (n 219) 10.

> moment, I would say that we have finished our work [on] norms. We will not introduce additional norms. So our whole attention for the second half of this year [(2019)] will go to principles, or wider picture [questions, i.e.,] what is cyberstability, and forms of future international cooperation in the field.[739]

In concurrence with its role as norm leader, the Commission has also acted as collaboration incubator and has, through its ideational efforts, established important bridges between different venues and stakeholders.[740] To illustrate, the proposed initiation of communities of interest to work collaboratively towards operationalisation and implementation of the normative prescriptions issued by the Commission also ranks among its collaboration-fostering endeavours.[741]

6.1.5 Effectiveness Review: Exerting Global Influence

This section evaluates the effectiveness of the norm creation activities undertaken by the Global Commission on the Stability of Cyberspace along the three dimensions introduced in *Chapter 3*: (a) output, (b) outcome, and (c) impact.[742] The GCSC's contributions to cybersecurity norm-making processes are rated along scales of high,

---

739 Interview #9 (n 445).

740 Interview #5 (n 731).

741 The GCSC's final report held that 'different organisations and members of society may be interested in advocating for certain norms more than others. ... Creating [c]ommunities of [i]nterest permits those having expertise in specific norms to work on their further development and implementation. For example, Computer Emergency Response Teams (CERTs/CSIRTs) may be particularly interested in implementing and monitoring the UN GGE norm aimed at protecting that community, just as those responsible for electoral systems may be particularly interested in the GCSC norm on electoral systems', see Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492) 25.

742 To recapitulate, the three effectiveness dimensions can be distinguished as follows: output refers to identifiable commitments and achievements set by actors engaging in global steering efforts. The latter can take the form of norms, standards and regulations, programs, as well as institutional structures. Performatively linked to output, outcome, denotes changes in the conduct of participating actors in accordance with the commitments stipulated. Impact relates to contributions to problem-solving resulting from the behavioural alterations of the stakeholders involved. While output and outcome facilitate analyses of non-state actor functions, impact enables differentiations between commitments and actions on the one hand and their larger effects on the other, see Wolf (n 340).

medium, and low across the three dimensions. For an overview of the different evaluation benchmarks, e.g. what does a medium rating along the dimension of outcome imply, please refer to Table 3.3 in *Chapter 2*.

Output

Over the course of its existence, the GCSC has issued respectable numbers of candidate norms, related commentaries, and research documents. Its frequent interactions with governmental and non-governmental stakeholders have allowed it to propose broadly supported and strategically-relevant normative ideas. Furthermore, its strong commitment to and encouragement of multistakeholder-oriented processes have helped strengthen perceptions that international peace and security need to follow pluralistic approaches. 'Cyberspace is a multistakeholder environment: those who build and manage cyberspace, and those who respond to attacks on and through cyberspace, are as likely to be non-state actors as government officials'.[743]

In terms of expanding global understandings of appropriate conduct in cyberspace for both state and non-state actors, the GCSC has benefited from deliberately and systematically linking its activities to other, preceding and ongoing, norm creation efforts, including

> the foundational ... work of the United Nations Group of Governmental Experts (UN GGE), the work of the Open-ended Working Group (UN OEWG), as well as the efforts of the Global Forum on Cyber Expertise (GFCE), [the] World Summit on the Information Society (WSIS), the Global Commission on Internet Governance ..., the Internet Governance Forum (IGF), the Global Conference on CyberSpace ..., the NETmundial Initiative, the Organization for Security and Co-operation in Europe (OSCE), the African Union Commission (AUC), the Charter of Trust, the Cybersecurity Tech Accord, [t]he Hague Program for Cyber Norms, the United Nations Institute for Disarmament Research (UNIDIR), the Paris Call for Trust and Security in Cyberspace ..., and the UN Secretary-General's High-level Panel on Digital Cooperation.[744]

---

[743] Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492) 7.

[744] Ibid 11-12.

The Commission's research publications as well as its outreach activities have served as important elements with regard to drawing attention to the ideational proposals of the Commission and other non-state actors more generally, and opening up conventional, mostly state-driven structures of debate. Renata Dwan, Director of the United Nations Institute for Disarmament Research, for example, has argued that

> [the GCSC] meetings [are] important because after being on the UN agenda for over two decades, we are now seeing an expansion on the discussion around what cyberstability means and for whom. A debate that began focused on state behaviour, is now becoming a much wider discussion about the role of the private sector, of regions and of individuals – and how to develop space for rights, for equity, and for access that enhances development for all.[745]

Apropos legitimising its endeavours, the Commission has benefited from a unique combination of technological know-how and expertise, access to relevant (political) networks, as well as public exposure of its commissioners.

With reference to the benchmarks developed as part of *Chapter 2*, the Commission has been highly effective in terms of producing and successfully advocating for normative standards that meet urgent global cybersecurity needs.

Outcome

The GCSC has successfully managed to insert its candidate norms into high-ranking regional and international policy-making processes, and affect actor behaviour. As a consequence of conscious advocacy activities by GCSC Commissioner and former Dutch Member of the European Parliament, Marietje Schaake, for instance, the GCSC's norm-making endeavours have been included in the cyberdefence report of the European Parliament (2018/2004)INI)). Paragraph 48 of the report as adopted

---

[745] Global Commission on the Stability of Cyberspace, Global Commission Convenes Fifth Cyber Stability Hearings at the United Nations, Geneva (2019) ⟨https://perma.cc/2ETD-KHQS⟩ accessed 10 February 2019.

by the European Parliament's Foreign Affairs Committee on 25 May 2018 states that the European Parliament supports

> the work of the Global Commission on the Stability of Cyberspace to develop proposals for norms and policies to enhance international security and stability and to guide responsible state and non-state behaviour in cyber[space]; endorses the proposal that state and non-state actors should not conduct, or knowingly allow, activity that intentionally and substantially damages the general availability or integrity of the public core of the internet, and therefore the stability of cyber[space].[746]

The European Union has also expressed clear commitment to the protection of the public core of the internet in the EU Cybersecurity Act. The preamble of the EU Cybersecurity Act reads:

> The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA [(the European Union Agency for Cybersecurity)] should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top level domains), and the operation of the root zone.[747]

Article five of the EU Cybersecurity Act further holds that

> ENISA shall contribute to the development and implementation of Union Policy and Law, by ... assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet.[748]

Private actors, too, have commended the activities of the GCSC. The Forum of Incident Response and Security Teams (FIRST), for instance, has recognised the

---

[746] European Parliament, *Report on Cyber Defence (2018/2004(INI))* (techspace rep, 2018) ⟨https://perma.cc/SLM9-HRVH⟩ para. 48.

[747] European Union (n 492) para. 23.

[748] Ibid art. 5, para. 3.

cooperation-oriented qualities of the Commission's endeavours: 'FIRST deeply values the work of the Global Commission on the Stability of Cyberspace, and applaud and support [its] efforts to promote mutual understanding between the various communities operating the internet'.[749]

The GCSC has also received mention in a UN Secretary-General report, which cited the Commission's efforts on norms of responsible behaviour for reducing the risks to cyberstability.[750] In November 2018, five of the Commission's eight candidate norms were recognised in the *Paris Call for Trust and Security in Cyberspace*. Signed by more than 1,000 stakeholders (both governmental and non-governmental), the Paris Call makes reference to the following ideational proposals of the GCSC: (a) the protection of the general availability and integrity of the public core of the internet, (b) the safeguarding of electoral infrastructures, (c) the responsibility of private actors in strengthening the security of digital processes, products and services, (d) the need for cyberhygiene as a foundational defence, (e) as well as the need to prevent non-state actors, including the private sector, from hacking back, for their own purposes or those of other actors.[751]

The inclusion of the GCSC's candidate norms into policy documents such as the Paris Call or the EU Cybersecurity Act as well as its far-reaching endorsement are evidence of the Commission's successfully executed roles as norm leader and cooperation incubator, and also speak to its capacity to prompt behavioural and institutional transformations.

---

749 FIRST Address to the Global Commission on the Stability of Cyberspace (n 735).

750 United Nations Economic and Social Council, Progress Made in the Implementation of and Follow-Up to the World Summit on the Information Society Outcomes at the Regional and International Levels (2019) ⟨https://perma.cc/FPF9-LMYR⟩ para. 65.

751 Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace (n 562); Global Commission on the Stability of Cyberspace, *Call for Contributions on the 2019 BPF on Cybersecurity: Submission of the Global Commission on the Stability of Cyberspace* (techspace rep, 2019) ⟨https://perma.cc/M8K8-3VG8⟩.

Impact

Questions concerning the extent to which activities of non-state actors, such as the GCSC, can impact larger systemic conditions are highly debatable, yet not misplaced. In other security-related areas, including the abolition of nuclear weapons, unilateral actions conducted by non-state actors have led to or been recognised for large-scale systemic improvements.[752]

In terms of enhancing international security and stability of the virtual realm, i.e. reducing or at least keeping constant the numbers of cybersecurity incidents and related costs, as well as the proliferation of offensive cybercapabilities, the Commission has not been as successful as it has been across the dimensions of output and outcome. Despite heightened levels of activities and normative stipulations made by the GCSC, offensive cyberoperations and attacks have not abated.[753] Arguably, it is difficult to establish direct performative links between the occurrence or non-occurrence of cybersecurity incidents and the norm-generating activities of the Commission. Also, it is still early to judge the long-term effects of the activities undertaken by the GCSC. Norms require time and concerted efforts for being adopted and implemented. However, it is critical to establish relevant tracking baselines as soon as possible which is what this manuscripts seeks to achieve. In a cautiously optimistic manner, Expert #6, for instance has noted that

> they [the Commissioners] are really diverse in terms of stakeholder composition. They have really great names [on board]. ... And they are really trying to ask for public comments. And I think that up to now, from

[752] See, for instance, International Campaign to Abolish Nuclear Weapons, ICAN Receives 2017 Nobel Peace Prize (2017) ⟨https://perma.cc/LR56-TMTF⟩ accessed 6 December 2019. In 2017, the International Campaign to Abolish Nuclear Weapons, a coalition of non-governmental organisations was awarded the Nobel Peace Prize for 'its work to draw attention to the catastrophic humanitarian consequences of any use of nuclear weapons and for its ground-breaking efforts to achieve a treaty-based prohibition of such weapons', see ibid.

[753] Center for Strategic and International Studies (n 4); Information is Beautiful, World's Biggest Data Breaches & Hacks (2019) ⟨https://perma.cc/K9PT-8S62⟩ accessed 6 December 2019.

> what I have seen [so far], it is probably the most promising and the most popularised initiative. I do not know if they [get] those norms and additions to fly and be implemented, but I think they really have great potential, and I think that they are a great group of people who are really trying to change something. And even if the Norm Package will die or will not be implemented, perhaps something [else] could be built upon their mistakes, and in that sense it is a great contribution either way.[754]

While, so far, the global state of cybersecurity has seen little improvement as a consequence of the Commission's norm-making undertakings, its efforts have increased levels of issue sensitivity and have had effects at substantive levels. Among other things, the GCSC's commitments to stipulating responsible behaviour in the digital environment have led to renewed emphases on the inclusion of civil society organisations and other private stakeholders in global cybersecurity problem-solving efforts. Furthermore, its activities have helped sustain and reinvigorate momentum for debates about rules of the road in cyberspace and the need for inclusive approaches (particularly so following the non-consensus outcome of the 2017 UN GGE). The GCSC's effects on putting issues of considerable urgency on 'the radar screens of policymakers and publics', and garnering ideational support across fora such as the European Union or the Paris Peace Forum should not be underestimated.[755] Moreover, the Commission has made substantive contributions to cybersecurity-related normative orders by introducing conceptual guidelines (frameworks), issuing complementary candidate norms for both state and non-state actors, and providing recommendations for further progress. All things considered, the Commission has not met all of the targets it set out to achieve, which may have been very aspirational, but has laid important foundations for guiding responsible interactions in cyberspace. Hence, in terms of goal attainment and impact, the GCSC has been partially effective.

---

[754] Expert #6, Interview #6 (2019).

[755] Evans (n 696) 289.

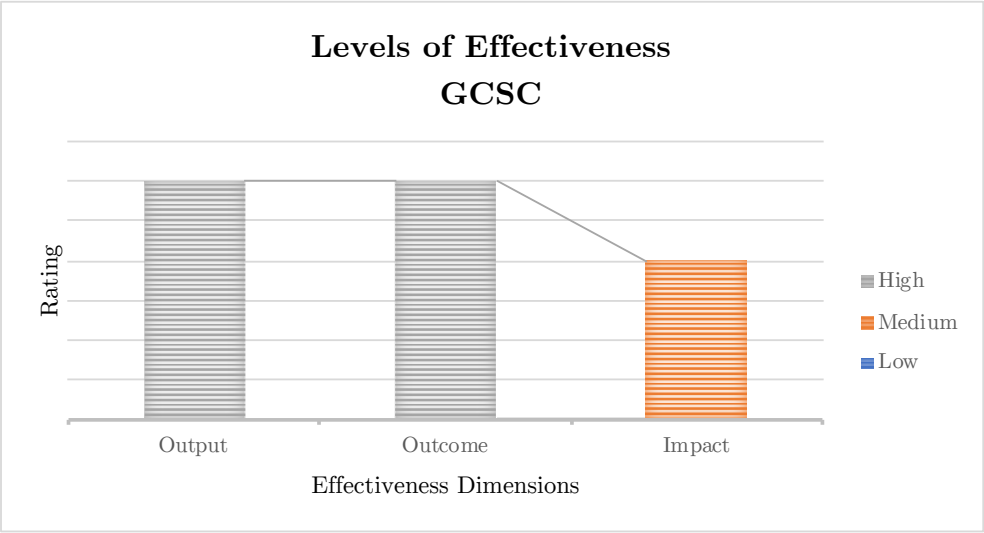

Figure 6.1: Effectiveness Plot: Global Commission on the Stability of Cyberspace.

6.1.6 Précis

This section has argued that the Global Commission on the Stability of Cyberspace has exerted discernible discursive and political power over discussions about responsible behaviour in cyberspace. It has made sensitising and substantive contributions. Reviewing the Commission's activities, this section has contended that the GCSC has executed three principal roles: (a) awareness raiser, (b) discussion feeder and gap filler, and (c) norm leader and cooperation incubator.

Its activities have been far-reaching, and its normative proposals well-crafted to resonate with diverse target audiences. Its meeting practices, i.e. holding gatherings at the sidelines of major cybersecurity conferences and preparatory intergovernmental sounding efforts, too, have constituted well-wrought strategic choices. To a certain extent, the Commission has taken on authoritative roles and regulatory functions previously ascribed to governmental entities, for instance, norm leadership.

However, while having been effective across the dimensions of output and outcome,

the Commission has struggled to enhance the overall stability and security of the virtual realm (impact). Despite heightened levels of activities and normative stipulations made by the GCSC, offensive cyberoperations and attacks have not abated nor have the proposed norms been meaningfully enforced. Notwithstanding the Commission's inability to effect broader systemic change, it 'has the potential to become a trusted source of inspiration for global internet policy-making in the 2020s'.[756]

	Output	**Outcome**	**Impact**
High	The Commission has issued respectable numbers of norms and has created an implementation-oriented cyberstability framework.	The Commission has effectuated changes in behaviour of targeted actors to the extent that they have issued policy commitments; Its norms have been referenced across other high-ranking international policy fora.	-
Medium	-	-	The Commission has made contributions to the normative order and has managed to maintain normative issues on international political agendas. Its efforts have, however, not yet led to noticeable reductions in the levels of cyberinstabilty.
Low	-	-	-

Table 6.4: Effectiveness Review: Global Commission on the Stability of Cyberspace.

If taken up appropriately, the efforts launched by the GCSC have the capacity to act as mould shells for more peaceful interactions in cyberspace. They are useful cornerstones for lining out and shaping the boundaries of acceptable conduct in the

[756] The Kaljurand Commission: Building Bridges Over Troubled Cyber-Water (n 728) 3.

virtual realm. Further progress towards widely accepted norms of responsible behaviour is likely to require time, as well as the 'simultaneous use of multiple arenas'.[757]

6.2 Forum of Incident Response and Security Teams: Providing Level-Headedness

In conjunction with the steep rise in malicious cyberattacks, incident response activities have acquired considerable international attention. Early efforts undertaken by computer security incident response teams (CSIRTs) to react to (then) large-scale computer security incidents in the late 1980s were seen to be lacking in coordination and consistency. Among other things, exchanges between CSIRTs were hampered by 'differences in language, time zone, and international standards or conventions'.[758] In reaction to these difficulties and the mounting importance to meaningfully respond to cybersecurity incidents, in 1990, the Forum of Incident Response and Security Teams (FIRST) was formed. The Forum of Incident Response and Security Teams is a North Carolina-based non-profit corporation of trusted international computer response teams, devoted to effectively reacting to 'security incidents by providing access to best practices, tools, and trusted communications with member teams'.[759]

6.2.1 Background: Extending Operational Horizons

What started as a small network of a few committed response parties has now grown into an international community of more than 520 response teams from commercial, government and academic sectors across more than 90 countries in the Americas, Asia,

[757] How Will New Cybersecurity Norms Develop? (n 728).

[758] Forum of Incident Response and Security Teams, FIRST History (2020) ⟨https://perma.cc/LVV9-988R⟩ accessed 28 August 2020.

[759] Forum of Incident Response and Security Teams, Bylaws of FIRST.Org, Inc. (2020) ⟨https://perma.cc/7WZT-C6S5⟩ accessed 28 August 2020.

Europe, Africa, and Oceania.[760] Since its inauguration in 1990, FIRST has 'resolved an almost continuous stream of security-related attacks and incidents'.[761] FIRST has become the largest global confederation of CSIRTs, and builds capability by facilitating events and workshops, and supporting its members in developing standards.[762] Given the nature of the activities conducted by the different teams, some commentators have compared CSIRTs and international associations of CSIRTs to 'digital fire brigades, centres for disease control, or digital Emergency Medical Technicians – first responders whose mission is to put out the fire, or to assess the situation and keep [victims] alive'.[763]

Organisationally, FIRST comprises a Board of Directors, an Executive Director, a Secretariat, as well as ad hoc and standing committees. The Board of Directors is made up of ten elected individuals and bears responsibility for managing the activities and affairs of the association as a whole. The Board of Directors also appoints the Chair and the Chief Financial Officer of FIRST.[764] The Board of Directors further 'establishes standing (permanent) and ad hoc (temporary) committees in order to better achieve FIRST's goals'.[765] In addition to being an administrative point of contact for prospective and existing members, the FIRST Secretariat maintains the membership database as well as the association's web and e-mail services.[766] The Executive Director position

760 For a complete list of incident response teams participating in FIRST, please consult Forum of Incident Response and Security Teams, FIRST Members (2020) ⟨https://perma.cc/FXG7-ASLE⟩ accessed 28 August 2020.

761 Forum of Incident Response and Security Teams, About FIRST (2020) ⟨https://perma.cc/3PDT-7NEX⟩ accessed 28 August 2020.

762 Forum of Incident Response and Security Teams, Education (2020) ⟨https://perma.cc/X8S9-8SNF⟩ accessed 28 August 2020.

763 Isabela Skierka and others, 'CSIRT Basics for Policy-Makers' (Washington, DC and Berlin, 2015) ⟨https://perma.cc/7JRM-P5M9⟩ 7.

764 Serge Droz serves as the current (as at April 2020) Chair of FIRST, see Forum of Incident Response and Security Teams, Board of Directors (2020) ⟨https://perma.cc/RW95-6YDS⟩ accessed 28 August 2020. A Chair can serve a maximum of two consecutive one-year terms.

765 Bylaws of FIRST.Org, Inc. (n 759).

766 Forum of Incident Response and Security Teams, Organisation (2020) ⟨https://perma.cc/H46L-BMEE⟩ accessed 28 August 2020.

is a recent addition to FIRST's organisational structure (as at May 2019).[767] The Executive Director closely collaborates with the Board of Directors to execute annual programmes and implement the organisation's strategic plan. The incumbent also completes public relations and fundraising mandates, as well as outreach activities.[768]

FIRST has two standing committees, a Membership Committee, and a Conference Program Committee. The former is concerned with all aspects of membership administration, including membership applications and reviews, recruitment and retention, as well as communications. The Conference Program Committee is in charge of programme development and speaker selections for FIRST's Annual Conference.[769] FIRST's Annual Conference serves as a meeting point for Computer Security Incident Response Teams and other interested parties to share 'goals, ideas and information on how to improve global computer security', and extend partnerships.[770] In addition to networking opportunities, the yearly convention also functions as a venue for education. Participants can learn about the latest incident response and prevention techniques as well as security strategies, develop their technical knowledge, and share best practices vis-à-vis managing incidents.[771] Education is central to FIRST's operational mission.

> Ensuring CSIRT teams are well trained is a prerequisite for FIRST to be successful in its mission. Security incidents rarely occur in isolation, and in order to effectively respond, incident responders need to be able to find viable partners in the network where the attack originates, or through which it transits.[772]

---

767 Chris Gibson, former Chief Information Security Officer of Orwell Group, ex-FIRST Board member, ex-FIRST Chief Financial Officer and ex-FIRST Chair has been appointed Executive Director, see Forum of Incident Response and Security Teams, Chris Gibson appointed Executive Director at FIRST (2019) ⟨https://perma.cc/N39N-N2VB⟩ accessed 28 August 2020.

768 Ibid.

769 Organisation (n 766).

770 Forum of Incident Response and Security Teams, 31st Annual FIRST Conference (2019) ⟨https://perma.cc/QQ7S-WMK2⟩ accessed 28 August 2020.

771 Ibid.

772 Forum of Incident Response and Security Teams, Education Programme (2020) ⟨https://perma.cc/AK3A-WNBG⟩ accessed 28 August 2020.

Besides the two standing committees, FIRST also houses a variety of Special Interest Groups (SIGs) which can take one of four forms, i.e. Working Groups, Standards Groups, Discussion Groups, or Bird of a Feather Groups. SIGs are composed of individual FIRST members and invited parties, who come together to explore an area of interest or specific field of technology, and collaborate and share expertise and experiences to address common challenges.[773] Examples of Special Interest Groups include, among others, Ethics SIG, Big Data SIG, or Information Sharing SIG.[774]

6.2.2 Mandate and Goals: Securing the Virtual Realm

With regard to its organisational mandate, FIRST aspires to be a trailblazer in the remit of incident response by providing access to best practices, tools, and trusted lines of communication among its members. It understands its mission to consist of three core areas, (a) fostering global coordination, (b) promoting a global language, and (c) engaging with policymakers and other relevant stakeholders.[775] With reference to the three goals outlined above, FIRST has implemented different training and education programmes, aimed at helping incident response teams streamline and standardise their processes and mature their operations.

---

[773] Forum of Incident Response and Security Teams, Global Initiatives (2020) ⟨https://perma.cc/HYX7-PTZZ⟩ accessed 28 August 2020.

[774] Ibid.

[775] FIRST's mission statement reads as follows: 'Global Coordination – You can always find the team and information you need: FIRST provides platforms, means and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture. Global Language - Incident responders around the world speak the same language and understand each other's intents and methods: During an incident it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine to machine communication. Policy and Governance - Make sure others understand what we do, and enable us rather than limit us: FIRST members do not work in isolation, but are part of a larger system. FIRST engages with relevant stakeholders, in technical and non-technical communities, to ensure teams can work in an environment that is conducive to their goals', see Forum of Incident Response and Security Teams, Mission Statement (2020) ⟨https://perma.cc/X2JR-425Y⟩ accessed 28 August 2020.

6.2.3 Activities: Complementing Existing Efforts

Since 1990, FIRST has held conferences, trainings and workshops for technical incident responders. In addition to its annual conferences, FIRST has set up *Technical Colloquia* and *Symposia*. Symposia are rotating regional one- to two-day assemblies of 100 to 300 attendees, which typically precede or follow FIRST members only, closed events. Symposia are often co-hosted by local event partners and in terms of content are less technical, and more practice-oriented in nature. In contrast, Technical Colloquia are dedicated gatherings of 'FIRST members and invited guests to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams'.[776] Compared to Symposia, Technical Colloquia are smaller, yet more frequent national/regional meetings. They are often led by experienced security professionals who educate participants on technical topics, such as incident forensics in an interactive manner.[777]

More recently, FIRST has supplemented its education efforts with training sessions on cybersecurity incident response for policymakers, policy analysts and government officials. These workshops seek to educate non-technical audiences on cybersecurity incident response and resilience strategies. Among other things, the half-day training session addresses elementary question such as: *What are Computer Security Incident Response Teams (CSIRT) and how did they come to exist? Why do they matter? What are typical functions of CSIRT? How do CSIRT enable and maintain cooperative setups across international boundaries and sectors? How are trusted relationships formed among incident responders?*[778] While, according to board member Maarten Van

[776] Forum of Incident Response and Security Teams, Technical Colloquia & Symposia (2020) ⟨https://perma.cc/KL4G-48D6⟩ accessed 31 August 2020.

[777] Forum of Incident Response and Security Teams, Technical Colloquia & Symposia (2020) ⟨https://perma.cc/698U-GETS⟩ accessed 28 August 2020.

[778] As at March 2020, FIRST has conducted four policymaker-oriented training sessions in Geneva (2017), New York (2018), Seoul (2018), and Tallinn (2019).

Horenbeeck, FIRST will primarily continue to provide and make accessible knowledge and insights to technical communities, the policymaker training is envisaged to broaden incident response addressees and support non-technical experts 'in making optimal policy decisions, enabling [FIRST] member teams to be more effective dealing with major cross-border security incidents'.[779]

FIRST's efforts to engage with non-technical communities are evidence that

> [CSIRTs] have come to form a key part of the complex regime of loosely coupled norms and institutions that govern cyberspace today. At the same time, CSIRTs are facing a tipping point. They are becoming increasingly part of the broader cybersecurity policy discussion and face the need and challenge to accommodate other policy and political objectives.[780]

Since 2017, FIRST has become an active participant and player in debates about cybersecurity governance. In the remit of international multistakeholder conventions, FIRST has helped organise information as well as best practice sessions concerning rules of the road for cyberspace via its board members. FIRST board member Maarten Van Horenbeeck, for instance, has served as Lead Expert for the United Nations Internet Governance Forum Best Practice Forum (BPF) on Cybersecurity since 2014. BPFs are multistakeholder-based intersessional programmes meant to produce concrete outputs, enhance the policy impact and reach of IGF meetings, and contribute to broader governance debates.[781] 'BPF outcomes – in the form of compilations of good practices – are intended to help inform policy debates and serve as inputs into other pertinent forums and processes'.[782] BPF contributions are typically solicited via in situ

---

779 Forum of Incident Response and Security Teams, FIRST Announces Incident Response Training for Policymakers (2017) ⟨https://perma.cc/Z5P9-QB5N⟩ accessed 28 August 2020.

780 Skierka and others (n 763) 7.

781 United Nations Internet Governance Forum, Best Practice Forums (2020) ⟨https://perma.cc/4VDQ-4SPL⟩ accessed 28 August 2020. BPF Cybersecurity Lead Expert Maarten Van Horenbeeck, for instance, presented key insights collected during the 2019 BPF on Cybersecurity at the UN Open-ended Working Group's informal intersessional consultative meeting with industry, academia, and NGOs on 2-4 December 2019 at the UN headquarters in New York, see United Nations Internet Governance Forum, IGF 2019 BPF on Cybersecurity Contributes to UN OEWG (2019) ⟨https://perma.cc/9DGA-L7QY⟩ accessed 28 August 2020.

782 Best Practice Forums (n 781).

discussions at the IGF, through surveys, virtual meetings, public consultations, as well as mailing list discussions.[783] The 2019 edition of the BPF on Cybersecurity looked at twenty different state and non-state-driven, global cybersecurity agreements with a view to identifying emerging best practices related to the implementation of published provisions, including principles, frameworks, and norms.[784] While the BPF report 'observed convergence points of different norms proposals and early signs of consensus on what is proper behaviour in cyberspace', it also noted that unless norm development processes are truly multistakeholder, pursue common goals, and are unambiguous in terms of the stipulations issued, further progress may be difficult to attain.[785]

In addition, FIRST has actively responded to calls for norms-related contributions. In the remit of the GCSC's Cyberstability Hearings held during the 2018 Singapore International Cyber Week, FIRST provided input vis-à-vis key challenges confronting the work of the GCSC from the perspective of CSIRTs. In his remarks to the Commission, Maarten Van Horenbeeck held that for norms-related implementation and cooperation efforts to be effective, trust among different stakeholders, but in particular among CSIRTs, is critical. Furthermore, he noted that the activities of security defenders should not be adversely affected by sanctions regimes, and that norm development and implementation processes should be guided by principles of inclusiveness and hard funding.[786] As is evident from the remarks above, FIRST's leadership has been critical for advancing and executing the organisation's norms-related activities.

---

783 Best Practice Forums (n 781).

784 A list of agreements considered for analysis by the 2019 BPF on Cybersecurity can be found on pp. 16-17 of its final report, see United Nations Internet Governance Forum, *Cybersecurity Agreements: Final BPF Output Report* (techspace rep, United Nations Internet Governance Forum 2019) ⟨https://perma.cc/VN5D-76P8⟩.

785 Ibid.

786 FIRST Address to the Global Commission on the Stability of Cyberspace (n 735).

6.2.4 Role Profiles: Forging Trust-Based Interactions Across Communities

In the context of promoting rules of the road for cyberspace, FIRST has taken on various different roles. It has simultaneously acted as awareness raiser, implementation assistant and capacity builder, as well as custom shaper.

Vis-à-vis its role as awareness raiser, the Forum has pursued a two-fold strategy. On the one hand, FIRST has boosted public understandings of its raison d'être and activities, on the other hand it has helped increase awareness about cybersecurity norms and responsible behaviour in cyberspace more generally. The Forum has consciously identified relevant venues for discussing cybersecurity norms-related issues, and has been a well-regarded and consistent contributor to international multistakeholder meetings receptive to these topics, including the UN IGFs.

Since its foundation, FIRST has gradually broadened the scope of its operations, and has moved from fairly narrow incident response activities to topics at the wider periphery of but closely related to incident response matters, including rules of the road for cyberspace. Expert #28, for instance, has noted that

> why we as FIRST would want to be involved [(in cybersecurity norms construction processes)], ... I think, is because we feel, as sort of the only global organisation of incident response teams, we can bring a lot of experiences and thoughts ... to the table. We have been in this game since the early 1990s. ... We have always been very narrowly focused on the incident response space, and to be fair, that is an area where we are trying to sort of expand out of. We found that because we have always been very at the coalface – we have been a very techie organisation with people who do incident response, so they are looking at ... packet captures, and they are doing techie stuff – ... we have been sort of buried away and hidden. And the rest of the world is not really aware of us. ... And we want to try and make sure that we are building the right environment for FIRST teams to flourish in. And I think that is where we are coming from right now. [Our board members] have done a lot of work in the last few years pulling us out of that *down in the coalface*, and trying to get us into this space where we can bring our experiences and competence ... to bear, to

> help people understand the right way forward. And contributing to norms, we think, is hugely beneficial.[787]

With regard to increasing awareness about its own activities, FIRST's policymaker trainings have been key vehicles for expanding the numbers of entities familiar with the organisation's efforts. Expert #27 has explained that

> since we have started this initiative, which was about three years ago, ... we [have gotten] a lot more feedback and a lot more awareness from state organisations that FIRST exists. For example, I will be at the Meridian Conference [(Meridian Process)], and FIRST will be there for the second time. And before that, there were no non-state actors ever present at these events.[788]

In terms of increasing the levels of visibility of cybersecurity norm construction processes, the organisation's IGF-based educational undertakings, especially board-member-led contributions to the Best Practice Forum on Cybersecurity, as well as its UN General Assembly First Committee-related policy submissions (UNGGE and OEWG) have formed part and parcel of the organisation's norms-based awareness raising activities. To illustrate, in the remit of Australia's *Public Consultation on Responsible State Behaviour in Cyberspace*, launched by the country's Department of Foreign Affairs and Trade in 2019, FIRST issued a position paper on cybersecurity developments within the UN context, in which it stressed the need for continuous awareness raising activities on the parts of states as well as capacity building and cooperation efforts to facilitate norms implementation.[789] It also lobbied for favourable policies relating to the work conducted by Computer Emergency Response Teams, and called on public

---

[787] Expert #28, Interview #28 (2019).

[788] Expert #27, Interview #27 (2019); Meridian, About Meridian (2020) ⟨https://perma.cc/FQ3A-KQCN⟩ accessed 28 August 2020.

[789] Forum of Incident Response and Security Teams, *Position Paper on Cybersecurity Developments Within the UN Context* (techspace rep, Australian Government Department of Foreign Affairs and Trade 2019) ⟨https://perma.cc/33HE-KN3Q⟩.

and private actors to 'adopt practical measures to create clear indications of the roles and responsibilities of their respective communities, to increase trust and capacity'.[790]

In conjunction with its awareness raiser role, FIRST has also acted as custom shaper. Its conferences, trainings, as well as exercises have allowed the Forum to share technical knowledge and exchange information but have also helped it ingrain principles-based approaches to cybersecurity, and initiate *community building processes*.[791] FIRST's draft Code of Ethics, entitled *EthicsfIRST*, has informed behavioural postures and processes across different areas of expertise. With regard to one of the duties listed in EthicsfIRST, i.e. engaging in vulnerabilities disclosure, Kaspersky Lab, for example, has noted that

> [w]e base our five principles [of vulnerabilities disclosure] on our more than 23 years of global work and continue to be inspired by some best practices and, in particular, the Forum of Incident Response and Security Teams' (FIRST's) Code of Ethics. In every case, we place top priority on the safety and security of our users (the people and organisations using Kaspersky products and solutions).[792]

When conducting trainings FIRST has been determined to respond to relevant community and capacity needs and has provided a suite of training materials at no/low costs for participants. By extending its training target groups to policymakers, in addition to governmental and non-governmental CSIRTs and PSIRTs, FIRST has contributed, among other things, to increasing levels of trust and capacity across different communities. Moreover, the organisation has helped advance, through its training and educational efforts, shared sets of normative and principled beliefs pertaining to incident response and responsible behaviour in cyberspace, more generally.[793]

---

[790] Forum of Incident Response and Security Teams, *Position Paper on Cybersecurity Developments Within the UN Context* (n 789) 3.

[791] Tanczer, Brass, and Carr (n 34) 62.

[792] Ethical Principles for Disclosing Vulnerabilities (n 676); Forum of Incident Response and Security Teams, EthicsfIRST: Ethics for Incident Response and Security Teams (2020) ⟨https://perma.cc/P95R-RQYQ⟩ accessed 28 August 2020.

[793] Tanczer, Brass, and Carr (n 34).

As fundamentally solutions- and remediation-oriented organisation, FIRST has also functioned as norms implementation assistant. Not only has it fostered collaboration and trust relationships across geographic, cultural, and political borders but it has also actively initiated operationalisation-guided policy endeavours relating to rules of the road for cyberspace. Its implementation assistant role pertaining to norms of responsible behaviour for the virtual realm, has been most evident in the context of the 2019 Best Practice Forum on Cybersecurity. By proxy, FIRST's norms operationalisation-oriented engagement has primarily been driven by board member and BPF Cybersecurity Lead Expert Maarten Van Horenbeeck.[794]

With regard to norms operationalisation, Van Horenbeeck has argued that if certain normative stipulations enjoy fairly broad support and advocates of norms-based initiatives have particular sets of 'experiences around the implementation' of some of these normative stipulations, then disseminating relevant practices and know-how can help processes of implementation cascade. Furthermore, shared examples of successful implementation are likely to increase norms-related adoption rates by other parties, and in turn strengthen levels of cybersecurity.[795] By focusing on implementation-related questions, FIRST has effectively responded to 'a lack of attention to how the substance of abstract norms is transformed and constructed' during phases of operationalisation, and how meaning is produced among different stakeholders.[796] From theoretical vantage points, the response mechanisms and practical techniques inherent to operationalisation processes offer possibilities for introducing elements of normativity which 'may depart from the intentions or normative objectives initially held by norm setters'.[797]

---

[794] The Operationalization of Norms and Principles on Cybersecurity (n 723).

[795] Ibid.

[796] Hendrik Huelss, 'After Decision-Making: The Operationalization of Norms in International Relations' (2017) 9(3) International Theory 381, 381.

[797] Ibid 404.

In terms of going about its implementation assistant role, FIRST has not only provided technical advice and expertise relating to norms of responsible behaviour in cyberspace but has actively sought to identify and further disseminate implementation-based best practices, thereby engaging across the full spectrum of operationalisation activities.[798]

6.2.5 Effectiveness Review: Crossing Boundaries

As the assessments of the activities and roles have shown, FIRST has moved beyond merely bringing together incident response and security teams and providing technical assistance. The organisation has promoted and emphasised shared best practices, enacted codes of conduct, and engaged normatively.[799] This section evaluates the success of the activities conducted by FIRST in the context of promoting shared standards of responsible behaviour in cyberspace along the three effectiveness dimensions specified earlier – output, outcome, and impact – and assigns ratings of high, medium, or low to the relevant dimensions.

Output

FIRST's norms-related engagements and publications have grown considerably since 2017. In large parts driven by its board members, FIRST has complemented its suite of community activities, including conferences, meetings, trainings, workshops, technical colloquia, symposia and social events with additional norms-oriented efforts across global policy venues, e.g. the United Nations Internet Governance Forum or the Open-ended Working Group. Its submissions and ideas presented at these fora have thereby been firmly embedded in its broader organisational mission, in particular

[798] The Operationalization of Norms and Principles on Cybersecurity (n 723); Forum of Incident Response and Security Teams, *Position Paper on Cybersecurity Developments Within the UN Context* (n 789).

[799] Tanczer, Brass, and Carr (n 34).

its goal to ensure other stakeholders understand the scope of its operations, and help the organisation thrive rather than putting spokes in its wheels.[800]

FIRST's publications as well as its norms-driven outreach activities have supported the establishment of critical links between members of technical communities and debates about norms of responsible behaviour, as well as between technical and non-technical stakeholders more generally. Technical stakeholders had little knowledge of the UN-driven cybersecurity norm formation processes prior to 2015. For instance, as per Expert #18, CERT members were largely unaware of the 2015 norm developed by the UN GGE which directly addressed them, and held that states should refrain from targeting CERTs of other states or use their CERTs to engage in 'malicious international activity'.[801]

FIRST's efforts in the context of promoting rules of the road for the virtual realm have helped increase awareness for FIRST's and CERTs' missions and mandates, and have underscored the convergence of technical and policy issues. Furthermore, FIRST's undertakings have provided important stimuli with regard to promoting issues concerning proliferation and operationalisation. In a public hearing organised by the Global Commission on the Stability of Cyberspace, FIRST board member Maarten Van Horenbeeck, for example, cautioned that

> [i]n terms of norms implementation, due to the wide and uncoordinated development of cybernorms, we [(FIRST)] see a risk that norms are being proposed which do not gain widespread support. We strongly encourage participants in this community to find creative ways to support and back norms implementation through hard funding. For instance, economic incentives can be created for states to protect the *core of the internet* by encouraging them to invest in efforts to harden critical software components. This discourages the investment in offensive technology against the core

---

800 Mission Statement (n 775).

801 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (n 26) 8.

> by making it more expensive and challenging. It will also discourage its widespread use.[802]

In line with the above, FIRST's efforts around promoting peace and security in cyberspace have displayed high output effectiveness. The organisation has seamlessly operated at and connected the interfaces of technology and policy. FIRST has usefully complemented its *standard* outreach activities with norms-based activities, and has helped identify areas of possible normative convergence and follow-through.

Outcome

As regards outcome, FIRST's normative efforts have been somewhat successful. The organisation has done much to elevate debates about rules of the road for cyberspace to the levels of technical communities, and has meaningfully integrated norms-oriented considerations into its own activities. By connecting technical and normative discussions, FIRST has laid important foundations for rectifying depictions of CERTs as 'mythical cure-all' creatures for cybersecurity issues and sensitising policymakers to the effects of norms-based undertakings on the operations of CERTs.[803] FIRST has effectively created spaces for technical and non-technical communities 'to engage and build an understanding of how each functions'.[804] Its efforts, however, have largely been confined to fora already familiar with norms, such as the UN IGF, or the Global Commission on the Stability of Cyberspace, and in consequence have addressed audiences generally receptive to normative ideas. Yet even in those norms-friendly circles, empirical data on how much these efforts have influenced the behaviours of third parties have been largely absent. As per Expert #28, assessing how successful FIRST's efforts have been is difficult.

---

[802] FIRST Address to the Global Commission on the Stability of Cyberspace (n 735) 2.

[803] Klée Aiken, Ready to Respond to the Cyber Norms Debate (2018) ⟨https://perma.cc/WP2E-C9RL⟩ accessed 28 August 2020.

[804] Ibid.

> They [(different audiences of FIRST's policymaker trainings and workshops)] have all gone away, saying thank you very much that has been useful. Have they delivered and done anything on it? – I genuinely do not think I know. And I think that is really where I would like to come in and be able to have metrics and have some insights. So, do we go back to them like, a year later [and ask]: ... Have you really changed your views on things since we have done it and how has that translated?[805]

Notwithstanding the absence of clear performance metrics, FIRST's undertakings apropos promoting rules of the road for cyberspace have had sensitising, structural, and procedural effects, in particular with regards to questions around norms implementation and operationalisation. Taking board member Maarten Van Horenbeeck's efforts in the remit of the Best Practice Forum on Cybersecurity as proxy markers of FIRST's normative endeavours, the activities undertaken by the BPF have received positive responses from members of the Cybersecurity Tech Accord. Signatories of the Cybersecurity Tech Accord have stated that

> [they] are ... delighted that the Internet Governance Forum's (IGF) Best Practice Forum on Cybersecurity has continued to build on its work from previous years by conducting invaluable research into initiatives dealing with the international aspects of cybersecurity. ... We believe that the attempt to map the most impactful initiatives is very valuable, and find that the analysis conducted so far provides an interesting overview of both the work on issues related to cybercrime and to international peace and stability.[806]

Impact

As an umbrella organisation of Computer Security Incident Response Teams, FIRST's activities have obvious links to the stability and security of the virtual realm. The integration of norms-oriented concerns into its undertakings have supported the

---

[805] Interview #28 (n 787).

[806] Cybersecurity Tech Accord, The Cybersecurity Tech Accord Response to a Call for Contributions from Best Practices Forum Working Group on Cybersecurity Culture, Norms and Values (2019) ⟨https://perma.cc/JC8R-VTKK⟩ accessed 28 August 2020.

organisation's overall vision to warrant stable and safe digital infrastructures for all, and have provided it with greater levels of exposure to policymakers.[807]

As per its own attestation, FIRST has handled 'thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing internet'.[808] In terms of goal attainment, entering into discussions about rules of the road for the virtual realm has allowed the confederation to deliver on the policy and governance elements of its mission statement. According to the 2019/2020 Chairman of the Board of Directors, Serge Droz, FIRST has matured organisationally as well as topically over the past few years. Apart from growing membership numbers, this has been evidenced by the fact that the organisation has 'been increasingly asked by policy-making bodies to advise on topics such as responsible vulnerabilities disclosure practices, capacity building and even norms of responsible state behaviour', and has further shown that FIRST is regarded as 'important stakeholder when it comes to global cybersecurity issues'.[809]

Through its targeted engagements and proposals across international policy venues and meetings, FIRST has acquired normative clout and influence. Rather than by means of political mandates, FIRST has derived its norms-oriented authority and standing from providing and usefully establishing connections to expert knowledge and experience in the areas of incident response and coordination. Concerning the levels of success yielded across the dimension of impact, FIRST's norms-oriented undertakings and interventions have had some effects on discussions about rules of the road for the virtual realm and related processes of norms implementation. The organisation's efforts have added useful degrees of level-headedness to cybersecurity norm formation debates.

---

807 About FIRST (n 761).

808 Ibid.

809 Forum of Incident Response and Security Teams, FIRST Releases Its 2019-20 Annual Report (2020) ⟨https://perma.cc/B973-H6T2⟩ accessed 28 August 2020.

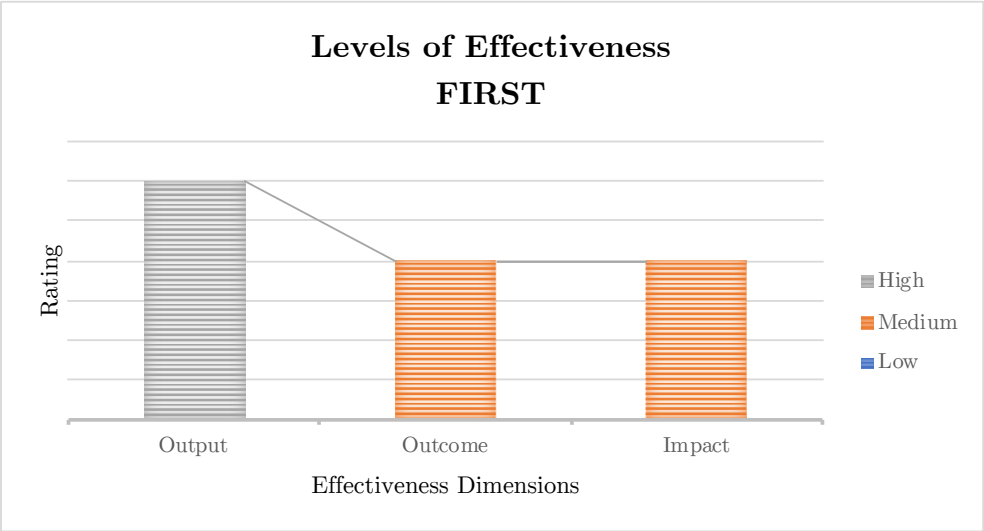

Figure 6.2: Effectiveness Plot: Forum of Incident Response and Security Teams.

To illustrate, as part of the interviews conducted, FIRST-associated Expert #12 maintained that

> [t]here are probably going to be very, very few norms that see any type of international enforcement. I think if you look at the UN GGE, for instance, the eleven norms that came out of their work, I could see there being meaningful agreement on those over the long-run, and there being some form of implementation, through for instance, sanctions agreements. I could see that happening, but we are still far away. I think where the short-term win for us lies in terms of enforcement is actually not so much enforcement, but it is really building out the capacity of organisations to implement the things that the norms actually prescribed. ... I think there is a big opportunity for states and enterprises to share the implementations that they are making to implement these norms in their business processes. And then as a result, they become a best practice and a catalyst for other organisations. Again, it would not stop someone from violating the norm intentionally, but it can help make the overall system more resilient, which is in the end with the internet the only thing we will ever get. We will never get to 100% norms implementation or enforcement the way we would not get to 100% cybersecurity.[810]

[810] Expert #12, Interview #12 (2019).

6.2.6 Précis

Surveying FIRST's efforts in the context of developing rules of the road for the virtual realm, this section has argued that the global umbrella organisation of more than 500 incident response teams has made positive normative contributions to advancing cooperation and security in cyberspace. It has supported discussions about norms of responsible behaviour in cyberspace both in sensitising, structural, as well as procedural terms. FIRST's board members have proven vital with regard to partaking in and submitting proposals to international norms venues and adding points of practical (security) reasoning to normative deliberations.

Apart from advancing knowledge about rules of the road for cyberspace across technical and non-technical communities, FIRST has used its ideational undertakings to raise awareness for its core activities 'to ensure [relevant] teams can work in an environment that is conducive to their goals'.[811] Furthermore, the Forum has acted as implementation assistant and custom shaper. Its implementation-focused activities have centred on questions of norms operationalisation and incentivisation of responsible behaviour. In promoting rules of the road for cyberspace, FIRST has benefited from its experiences in establishing trusted partnerships across technical communities, and has expanded shared sets of normative and principled beliefs pertaining to incident response and responsible behaviour across governmental and non-governmental circles by means of technical know-how and expertise. FIRST's norms-oriented efforts have been fairly successful across all three effectiveness dimensions, and, given the nature and scope of the organisation's activities and membership, have the potential to contribute even more significantly to stability and security in the virtual realm going forward.

FIRST's endeavours are prime examples of how highly specialised, technical expert groupings can contribute to policy projects and develop best practices in ways

[811] Mission Statement (n 775).

	Output	Outcome	Impact
High	FIRST's publications as well as its norms-oriented outreach activities have supported the establishment of critical links between members of technical communities and debates about norms of responsible behaviour, as well as between technical and non-technical stakeholders more generally.	-	-
Medium	-	FIRST's undertakings apropos rules of the road for cyberspace have had sensitising and procedural effects, in particular with regard to questions around norms implementation and operationalisation.	FIRST's interventions have had effects on discussions about rules of the road for the virtual realm and related processes of implementation. The organisation's efforts have added useful degrees of level-headedness to cybersecurity norms debates.
Low	-	-	-

Table 6.5: Effectiveness Review: Forum of Incident Response and Security Teams.

political actors cannot, namely by applying their knowledge practically, 'mobilising their expertise and overcoming disparities' when addressing cybersecurity issues of global proportions.[812] Analyses of the policy-oriented activities conducted by technical communities provide useful lenses through which 'to examine how international cooperation can move forward' and identify avenues for further progress, i.e. by focusing on areas of mutual, overlapping interests, and 'emphasising common ground

[812] Tanczer, Brass, and Carr (n 34) 64.

over differences' when tackling global cybersecurity matters.[813]

6.3 Carnegie Endowment for International Peace: Trailing Issue-Centericity

Along with increasing speeds and amounts of information, as well as ever more complex international relations, specialised information-processing entities, commonly referred to as think tanks, have come to take on important policy-guiding functions. These engagement and research institutes have responded to politicians' and bureaucrats' mounting needs for reliable, in-depth, and systematic analyses of domestic and international issues. Campbell and Pederson have argued that think tanks are sense-making apparatuses, i.e. 'knowledge-based regimes', which help address policy-relevant issues characterised by high degrees of uncertainty and ambiguity.[814] Sense-making processes are often 'contested ... involving varying degrees of competition, negotiation, and compromise – often involving power struggles – over the interpretation of problems and solutions for them'.[815] Think tanks assist in resolving these struggles by providing relevant platforms for debate and intellectual argument.[816]

Structurally, think tanks can display different degrees of affiliation and institutionalisation, i.e. from being ad hoc collections of issue-specific analysts to being permanent institutions, and from having close ties to sponsoring entities to enjoying complete independence. By virtue of their raison d'être, think tanks

> often act as a bridge between the academic and policy-making communities and between states and civil society, serving in the public interest as an

---

813 Tanczer, Brass, and Carr (n 34) 64.

814 McGann, *Think Tanks, Foreign Policy and the Emerging Powers* (n 693); John L Campbell and Ove K Pederson, *The National Origins of Policy Ideas: Knowledge Regimes in the United States, France, Germany, and Denmark* (Princeton University Press 2014).

815 Campbell and Pederson (n 814) 3.

816 Ibid.

> independent voice that translates applied and basic research into a language that is understandable, reliable, and accessible for policymakers and the public.[817]

As technology-based issues have come to figure on the agendas of world leaders and shape doctrines, think tanks have started to actively analyse trends and offer advice in the areas of cybersecurity and Artificial Intelligence, among others. One example of a leading global, technology-oriented think tank is Carnegie Endowment for International Peace.[818]

6.3.1 Background: Advancing Cooperation Globally

Carnegie Endowment for International Peace (short Carnegie Endowment) was founded in 1910 with a view to 'advancing cooperation between nations and promoting active international engagement by the United States'.[819] Carnegie Endowment is a private, non-profit, non-partisan think tank, housing approximately 140 analysts and scholars, dedicated to attaining practical results. Divided into ten programmes, i.e. Asia; Cyber Policy Initiative; Democracy, Conflict, and Governance; Europe; Geoeconomics and Strategy; Middle East; Nuclear Policy; Russia and Eurasia; South Asia; and Technology and International Affairs, it 'offers decision makers global, independent, and strategic insight and innovative ideas that advance international peace'.[820] In addition to Washington DC, Carnegie Endowment has offices in key policy hot-spots around the globe, including Beijing, Beirut, Brussels, Moscow, and New Delhi.

---

817 James G McGann, *Democratization and Market Reform in Developing and Transitional Countries: Think Tanks as Catalysts* (Routledge research in comparative politics, Routledge 2010) 1.

818 The 2019 Global Go To Think Tank Index Report, authored by James G. McGann, ranked Carnegie Endowment for International Peace second in the category of *Top Foreign Policy and International Affairs Think Tanks*, see James G McGann, *2019 Global Go To Think Tank Index Report* (techspace rep, University of Pennsylvania 2019) ⟨https://perma.cc/52T5-EFJF⟩ 134.

819 Carnegie Endowment for International Peace, About Carnegie (2020) ⟨https://perma.cc/3392-WSNC⟩ accessed 28 August 2020.

820 Ibid.

To sustain its operations, Carnegie Endowment for International Peace relies on financial donations from corporations, governments, foundations, as well as individuals who support its programmes.[821] As per information contained in its annual report, the think tank 'has reached new heights year after year in grants raised from the world's leading foundations, governments, and corporate donors, including a record USD 16 million in 2019'.[822]

6.3.2 Mandate and Goals: Furthering International Peace and Security

Congruent with its founder's intentions to advance peaceful international relations, Carnegie Endowment 'seeks to inject local perspectives into policy debates; prevent and mitigate collisions of global consequence; speed up the global policy response to technological, political, and economic transformations; and support new thought leaders in international affairs'.[823]

In furtherance of its mission to support international peace and security, Carnegie Endowment has employed different engagement instruments. Among other things, it has conducted research, published policy reports and papers, organised seminars, and contributed to conferences. With regard to networked technologies, it has also worked to 'help the development of international norms and rules of the road catch up to the pace of technological innovation-seeking to maximise the promise of new technologies while minimising their disruptions'.[824] Under the roof of the *Cyber Policy Initiative*,

[821] As per end of year 2019, Carnegie Endowment's net assets amounted to USD 340,671,353. One of the largest gifts received in 2019 was issued by Carnegie Endowment's Chair of the Board of Trustees, former US Secretary of Commerce, Penny Pritzker. Penny Pritzker made an USD 11 million pledge to Carnegie Endowment, which represented the single largest individual donation in the think tank's history, see About Carnegie (n 819).

[822] Carnegie Endowment for International Peace, '2019 Annual Report' [2020] 2019 Annual Report ⟨https://perma.cc/Q6XF-D3ZZ⟩.

[823] Ibid.

[824] Bill Burns, Carnegie Endowment for International Peace (2020) ⟨https://perma.cc/42K7-FB6S⟩ accessed 28 August 2020.

Carnegie Endowment has analysed key developments pertaining to cyberstrategy and -stability, and has sought engagement with high-level decision makers and experts.

6.3.3 Activities: Aggregating Insights and Issuing Proposals

The Cyber Policy Initiative has been an active contributor to cybersecurity norms-related discussions since at least 2015 and has focused on conducting hands-on research and issuing actionable policy proposals relating to cybersecurity norms. Participating in and commenting on key norm development processes across fora such as the G20 and the UN, the Cyber Policy Initiative has released mapping tools and published concrete normative proposals. Its *Cyber Norms Index* has been an example of the former, while its work pertaining to the implementation of a *Global Norm Against Manipulating the Integrity of Financial Data* has served as an illustration of the latter. The Cyber Norms Index is a repository of expressions of standards of appropriate behaviour in cyberspace issued by states between 2007-2017. The web-based index allows users to screen multilateral outcome documents for key words and compare specific language used across these documents by pre-defined categories.[825]

The Initiative's efforts relating to the implementation of a Global Norm Against Manipulating the Integrity of Financial Data have been informed by and benefited from its (active) engagement with governments and commercial actors, particularly in the remit of the G20, as well as its broader intentions vis-à-vis shaping and promoting feasible norms against malicious cyberactivities by state and non-state actors. Following earlier meetings with high-ranking policy stakeholders, and in response to comments issued by the G20 finance ministers and central bank governors around much-needed 'improvements in the resilience of the global financial system', Carnegie Endowment

[825] Carnegie Endowment for International Peace, Cyber Norms Index (2017) ⟨https://perma.cc/EV2T-4BXQ⟩ accessed 9 November 2017. The search categories include *International Law and Norms*, *Confidence and Capacity Building*, *Threat Perception*, and *Process*.

outlined next steps towards more formal and widely shared standards of behaviour pertaining to the protection of the global financial system against cyberthreats.[826]

In a white paper issued by Carnegie Endowment researchers Tim Maurer, Ariel Levite, and George Perkovich in 2017, the latter maintained that given the high degrees of interdependence among nations, the protection of the integrity of data and algorithms of financial institutions in times of peace and conflict is of paramount importance.[827] Apropos ensuring financial stability, they suggested the G20 finance ministers and central bank governors adopt explicit language prohibiting offensive cyberoperations against financial infrastructures along the following lines:

> A State must not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms wherever they are stored or when in transit. To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate activities manipulating the integrity of financial institutions' data and algorithms when such activities are passing through or emanating from its territory or perpetrated by its citizens.[828]

In phrasing and conceptualising the normative stipulations outlined above, the authors intended to offer (more concrete and tangible) specifications of earlier provisions issued around the protection of critical civilian infrastructures in the 2015 UN GGE and G20 communiqués. Given the strong and shared interests by governments as

---

826 Tim Maurer, Ariel Levite, and George Perkovich, 'Toward a Global Norm Against Manipulating the Integrity of Financial Data' (Washington, DC, 2017) ⟨https://perma.cc/SMH6-WWT7⟩.

827 The focus on protecting the integrity (emphasis added) of financial data (as opposed to confidentiality, for instance) was informed by a 2017 study published by the Massachusetts Institute of Technology, which held that '[o]ur economy is based on a system of accounts recording who owes what to whom at any moment. Those accounts are digitised, and so are back-up systems. An attack that destroyed or corrupted the accounts of a major financial institution could wreak devastating economic havoc unless those accounts could be quickly and reliably reconstituted. The risk extends beyond banks to securities exchanges, brokerage firms, investment companies, clearing organizations, and other financial enterprises. … A subtle, … operation that corrupted the pricing of selected securities, for example, could be used to manipulate markets, create illegal profits and losses, and drive parties out of business', see Joel Brenner, *Keeping America Safe. Toward More Secure Networks for Critical Sectors* (techspace rep, Massachusetts Institute of Technology 2017) ⟨https://perma.cc/UJ27-JE4Y⟩ 33.

828 Maurer, Levite, and Perkovich (n 826) 4.

well as international financial entities in safeguarding global asset flows, the authors considered moves towards normative alignment possible and within reach. According to Maurer and others '[s]tates [had] already demonstrated significant restraint from using cybermeans against the integrity of financial institutions' data'.[829] Hence, pledging allegiance to a Global Norm Against Manipulating the Integrity of Financial Data would cement already existing or emerging practices, and further strengthen confidence among states, they argued.

With the intention of further scaling its efforts and building support for its normative activities, Carnegie Endowment's Cyber Policy Initiative, in collaboration with the World Economic Forum, has launched a multi-year project, seeking to generate strategic and coherent insights vis-à-vis safeguarding the financial system against malicious cyberthreats, the FinCyber Strategy Project.[830] As part of initial agenda-setting efforts relating to the project, Carnegie Endowment organised a meeting with 50 seasoned professionals from governments, central banks, and business enterprises at Wilton Park, a UK-based refuge for strategic discussions of global scale, in July 2019. The meeting resulted in an initial work plan and six key strategic pillars. The six thematic priorities identified as part of the retreat included:

> (a) Operational resilience and the efforts of central banks, financial authorities, and industry;
>
> (b) Collective action by governments and industry to deter malicious cyberactivity targeting financial institutions;
>
> (c) International norms and diplomatic processes to increase cyberstability;
>
> (d) International capacity-building for governments and financial institutions;
>
> (e) Financial inclusion and how the leapfrogging to digital financial services can be protected and leveraged to advance basic cyberhygiene awareness;

---

[829] Maurer, Levite, and Perkovich (n 826) 4.

[830] Carnegie Endowment for International Peace, About the FinCyber Strategy Project (2020) ⟨https://perma.cc/ZJ2K-RLAY⟩ accessed 28 August 2020.

(f) Skills development to address the growing shortage in the cybersecurity workforce.[831]

The research and policy work scheduled to be undertaken by the Cyber Policy Initiative around these six pillars is supported by an eminent advisory group consisting of senior business leaders, international representatives from central banks as well as government envoys.[832]

6.3.4 Role Profiles: Brokering Ideational Know-How

In terms of contributing to cybersecurity norms-related discussions, Carnegie Endowment's Cyber Policy Initiative has brokered knowledge, actively issued and promoted normative contents (centred around financial stability) and boundary objects, and sought diplomatic engagement. As a leading global think tank for international affairs, the knowledge broker role has been one of the more evident roles assumed by the Initiative. With regard to cybersecurity norms, the organisation has pursued sequential strategies, and has gradually extended the types of functions executed. i.e. the role as knowledge broker has preceded the think tank's role as norm leader. The Cyber Norms Index has served as one of several *boundary objects* released by the Initiative.[833] In addition to the publication of the Index, the Cyber Policy Initiative has regularly published cybersecurity norms-related reports and blog posts, and has hosted multistakeholder-driven events.[834]

Apart from its knowledge broker role, the initiative has also drafted and called for the adoption of concrete normative proposals. With the intention of aiding the

831 About the FinCyber Strategy Project (n 830).

832 ibid. Please consult *ibid* for a list comprising the members of the advisory group.

833 Bandola-Gill and Lyall (n 441).

834 Carnegie Endowment for International Peace, International Cybersecurity Norms (2020) ⟨https://perma.cc/P7TP-YKU3⟩ accessed 28 August 2020 provides a list of relevant publications and events.

operationalisation of the 2015 UN GGE norms, in particular as they regard the protection of critical civilian infrastructure, the Cyber Policy Initiative has called for states 'not to undermine the integrity of data and algorithms of financial institutions in peacetime or during war, nor to allow their nationals to do so'.[835] According to Maurer and others,

> the integrity of financial institutions' data can, intentionally and/or unintentionally, threaten financial stability and the stability of the international system. Importantly, unlike the 2007-2008 global crisis, this risk exists independent of the underlying economic fundamentals and will only increase as more and more governments make cashless economies an explicit goal.[836]

The authors of the provisions further argued that considerations relating to data integrity trump concerns of availability and confidentiality as the international consequences resulting from data manipulation 'are greater than violations of confidentiality and more difficult to address technically than the interruption of availability'.[837]

With a view to accelerating cybersecurity norms implementation rates and offering potential precedents for further normative progress, the Cyber Policy Initiative has sought to entice the world's leading economies to commit to its proposed stipulations. To this end, it has produced written outputs addressed to the G20 finance ministers and central bank governors, and has actively engaged with G20 penholders during public and private meetings, in particular during the German G20 presidency in 2017.[838] Through pursuing concrete policy goals at the international level, and approaching and entering key political venues, such as the G20, the think tank has effectively acted as diplomatic change agent. In furtherance of its normative proposals, the Initiative has, apart from the G20 political leaders, interacted and partnered with the International

---

835 Maurer, Levite, and Perkovich (n 826) 3.

836 Ibid 3.

837 Ibid 8.

838 Expert #32, Interview #32 (2020).

Monetary Fund, the SWIFT Institute, the Financial Services Information Sharing and Analysis Centre (FS-ISAC), JP Morgan Chase, as well as other leading financial institutions, and has conducted high-ranking policy meetings at historically portentous locations.[839] In conjunction with its diplomatic engagement it has also released a financial resilience-oriented capacity-building tool box, which is intended to aid small- and mid-sized enterprises as well as organisations with low levels of cybermaturity 'enhance their own security as well as that of their customers and third parties'.[840]

In terms of ideational content and thematic focus, the Initiative's co-director, Tim Maurer, has been instrumental in crafting and advancing the think tank's proposals. As a German national with close ties to the US, he has been uniquely positioned to engage with the G20 representatives during Germany's presidency and introduce relevant normative proposals.

6.3.5 Effectiveness Review: Developing Long-Term Strategies

For more than 100 years, Carnegie Endowment has sought to promote research efforts capable of impacting real world outcomes. This section evaluates the think tank's cybernorms-related endeavours launched in the 2010s across the dimensions of output, outcome and impact, and classifies them as either low, medium, or high. As per the Initiative's own attestation, it has actively intended to contribute to 'greater stability and civility in cyberspace', hence evaluations of the levels of effectiveness yielded serve as important and informative checkpoints for current and future ventures.[841]

---

[839] Carnegie Endowment for International Peace, Cyber Resilience and Financial Organisations: A Capacity-Building Tool Box (2020) ⟨https://perma.cc/CY9H-G9MR⟩ accessed 28 August 2020.

[840] The toolbox comprises artefacts including executive-level cybersecurity guides and checklists, as well as a comprehensive, supplementary report, see ibid.

[841] Carnegie Endowment for International Peace, Cyber Policy Initiative (2020) ⟨https://perma.cc/B5LT-JBHJ⟩ accessed 28 August 2020.

Output

In line with the core functions of research-oriented policy institutes and consistent with the activities surveyed above, the Cyber Policy Initiative has produced considerable numbers of practice-oriented research artefacts, including blog posts, policy papers, as well as journal articles and books. In addition, the Initiative has regularly enlisted senior government and industry officials to engage in exchanges on recent developments in debates about rules of the road for cyberspace, and has hosted and attended relevant (international) round tables and conferences to move discussions forward. Among the written and publicly available outputs, the Initiative's Cyber Norms Index, for instance, has served as a useful one-stop-shop for offering an overview of relevant bi- and multilateral cybersecurity norms processes, their contents, as well as cross-references to other texts. Information contained in the Cyber Norms Index has been referenced in publications of leading policy venues, including the 2018 report of the Munich Security Conference.[842]

Guided by considerations of implementability and issue-specificity, the Initiative's efforts launched vis-à-vis protecting the financial system against cyberthreats have constituted important engagement elements for interactions and partnerships with the World Economic Forum, leading technology consultancies and services providers, supervisory authorities, banks and insurers, as well as international conferences.[843] The Initiative's undertakings have laid the ideational groundwork for 'more long-term, coherent vision[s] for how to protect the financial system against cyberattacks'.[844] Conscious of prior norm formation projects, the Initiative has explicitly sought to amplify and bolster the effects of existing endeavours, while 'strengthen[ing] the

[842] Munich Security Conference, *Munich Security Report 2018* (techspace rep, Munich Security Conference 2018) ⟨https://perma.cc/4V6C-M6Z5⟩; Cyber Norms Index (n 825).

[843] About the FinCyber Strategy Project (n 830).

[844] Ibid.

connective tissue between them', and offering concrete suggestions for operationalising cybersecurity norms.[845]

Conceptually based on the March 2017 Communiqué of the G20 Finance Ministers and Central Bank Governors, the FinCyber Strategy Project has been firmly integrated into and become a key part of the Initiative's larger operational strategy.[846] Comprising different work streams, the Initiative's project-related policy endeavours have sought to ensure the actionability of its suggestions, namely to

> (a) send a clear signal that the stability of the global financial system depends on preserving the integrity of financial data in peacetime and during war and that the international community considers the latter off limits; (b) build confidence among states that already practice restraint in this domain, and thereby increase their leverage to mobilise the international community in case the norm is violated; (c) create political momentum for greater collaboration to tackle non-state actors who target financial institutions with cyber-enabled means; and (d) complement and enhance existing agreements and efforts, namely the 2015 G20 statement, 2015 UNGGE report, and the 2016 cyber guidance from the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO).[847]

Apropos output effectiveness, the contributions made by the Cyber Policy Initiative have been substantial. They have been tied to specific normative proposals, linked to the concerns of leading policy venues, and made part and parcel of the Initiative's operational priorities.

Outcome

With regard to stimulating changes in behaviours of governmental and non-governmental stakeholders apropos responsible conduct in cyberspace, the Carnegie Cyber Policy

---

845 About the FinCyber Strategy Project (n 830).

846 G20, *Communiqué G20 Finance Ministers and Central Bank Governors Meeting* (techspace rep, G20 2017) ⟨https://perma.cc/M9SC-XFXZ⟩.

847 Carnegie Endowment for International Peace, G20 Proposal (2020) ⟨https://perma.cc/DEC3-T93R⟩ accessed 28 August 2020.

Initiative has benefited from having access to leading international (economic) fora, such as the G20. Moreover, in seeking to seed the idea of a Global Norm Against Manipulating the Integrity of Financial Data, the Initiative has strategically grafted its proposals onto existing policy statements, e.g. the March 2017 Communiqué of the G20 finance ministers and central bank governors, and (allegedly) existing postures of restraint in relation to employing cyberattacks against the integrity of financial institutions' data. Doing so has allowed the Initiative to secure endorsements and cooperative arrangements with key players concerned with international economic relations. According to Expert #32, the Initiative has considerably influenced the German thinking around cybersecurity and the financial system during Germany's G20 presidency in 2017.[848]

Notwithstanding the wide range of pro-forma endorsements received from leading financial actors, or the targeted activities undertaken during Germany's G20 presidency, the Carnegie Cyber Policy Initiative has not succeeded at eliciting comprehensive and explicit commitments concerning its ideational suggestions from the G20 members, or the members of the FinCyber Strategy Project's advisory board for that matter, other than their approval to contribute to the FinCyber Strategy Project by means of sitting on the project's advisory board. Hence, despite well-positioned, and well-regarded ideational proposals, behavioural changes even among the Initiative's target audiences have so far remained in their infancy. Thanks to the Initiative's knowledge-brokering and engagement efforts, levels of appreciation for issues pertaining to financial stability and cybersecurity resilience have increased among the participants targeted, however, extensive shifts in their principled beliefs which define their interests, goals, and preferences, have not been readily observable or promoted publicly, e.g. by means of references to efforts launched by the Cyber Policy Initiative, publicly available commitments presented on websites, or relevant reports issued.

---

[848] Interview #32 (n 838).

Even though far-reaching behavioural adjustments have not taken hold as of yet, the Initiative's undertakings are well positioned for stimulating behavioural alterations in the long run. The Carnegie Cyber Policy Initiative's endeavours have been clear-cut, have shown high degrees of implementability, and have generally been well-received by target audiences. The Initiative's ambitions to collect and share best practices across different stakeholder groups may prove to be valuable trajectories for obtaining explicit normative commitments from relevant governmental and non-governmental stakeholders. So far, however, the Carnegie Cyber Policy Initiative's activities have had only average effects on the behaviours of its target audiences.

Impact

In contrast to behavioural changes which focus on conduct-related alterations of relevant target groups, structural changes take into account effects on third parties and broader political, legal, and social environments.[849] Akin to what has been observed vis-à-vis outcome, the norms-related efforts conducted by the Carnegie Cyber Policy Initiative have only yielded fair results in terms of systemic impact. Although attributions of causality are challenging to make, global levels of cybersecurity, and especially across the financial sector, have hardly seen any improvement as a result of the Initiative's projects or proposals. Given that the think tank has only just started its work on developing an *International Strategy for Cybersecurity and the Global Financial System*, and taking into account that explicit policy commitments from state actors and resulting systemic effects (e.g. in the remit of the G20) usually have extensive lead times, the limited systemic contributions should come as no surprise.[850]

What the Initiative has been successful at and where impact-related effects have been more tangible is at suggesting additions and specifications to cybersecurity norm

[849] Flohr and others, *The Role of Business in Global Governance* (n 219).

[850] About the FinCyber Strategy Project (n 830).

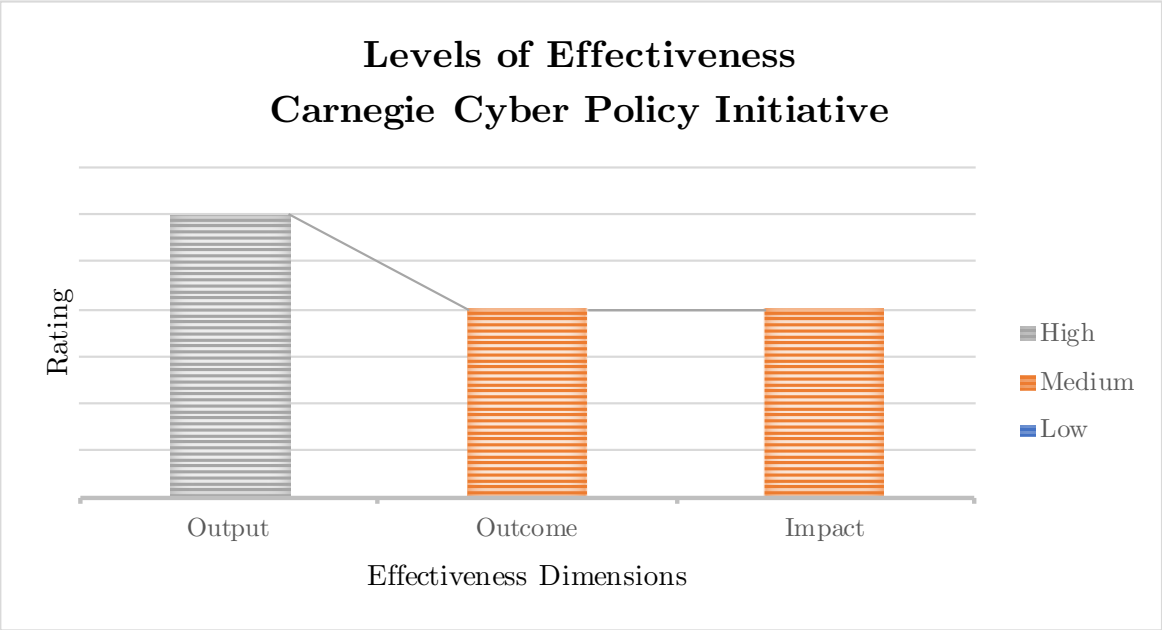

Figure 6.3: Effectiveness Plot: Carnegie Endowment Cyber Policy Initiative.

formation projects, thereby strengthening cybersecurity-related ideational textures. The Initiative's proposals to zoom in on the global financial system and specify norms relating to critical infrastructure protection, as for instance contained in the 2015 UN GGE report, have constituted useful add-ons to normative regimes in the virtual realm. Indeed, resulting from its diplomatic engagement, the Initiative's efforts have paved the way for future dedicated and unambiguous normative commitments from leading governmental and non-governmental stakeholders. Strategically tying its proposals to voiced concerns of policymakers has allowed the Initiative to garner support for and promulgate further ideational concepts to audiences not necessarily familiar with global cybersecurity norm formation projects, including e.g. financial institutions such as JP Morgan Chase, BNP Paribas, or Zurich Insurance Group.

The Carnegie Cyber Policy Initiative has usefully employed its track record of discretely facilitating 'policy development and reconciliation among diverse governmental and industrial stakeholders', has crossed conceptual and organisational boundaries, identified tangible areas of implementation, and moved discussions about rules of the

road for cyberspace forward.[851] With regard to its mission statement, the Initiative has delivered on its mandate to the extent that it has 'develop[ed] and promot[ed] norms and policy recommendations for enhancing international stability and security in cyberspace' but has so far had limited success vis-à-vis effectively reducing the numbers of international cyberpolicy challenges, or achieving greater stability and civility in cyberspace, respectively.[852]

6.3.6 Précis

This section has studied the norm formation endeavours undertaken by Carnegie Endowment's Cyber Policy Initiative. It has argued that the Initiative, in line with its policy-oriented origins, has made important substantive as well as sensitising and structural contributions to debates about rules of the road for cyberspace. As a norm leader it has crafted targeted and highly issue-driven ideational proposals and has brokered these across leading policy venues, including the G20, effectively taking on quasi-diplomatic functions. It has also used high-ranking dialogue venues, such as Wilton Park, to deliberate about longer-term strategic efforts vis-à-vis increasing the cyberstability and security of the global financial system.

Although its proposals have been clear-cut, and generally well received according to information provided by Expert #32, the Initiative has not yet managed to elicit explicit normative commitments from its target audiences.[853] Hence, in terms of levels of effectiveness achieved across the dimensions of outcome, and impact, the Initiative has only partially succeeded at changing actor behaviour and effecting systemic alterations. Grounded in research-oriented approaches, its activities have, however, produced considerable numbers of well-argued and informative policy artefacts. Despite lacking

---

851 About the FinCyber Strategy Project (n 830).

852 Ibid.

853 Interview #32 (n 838).

	Output	Outcome	Impact
High	The Cyber Policy Initiative has produced considerable numbers of practice-oriented research artefacts. Its efforts launched vis-à-vis protecting the financial system against cyberthreats have constituted important engagement elements for interactions and partnerships with leading international institutions and conferences.	-	-
Medium	-	Though behavioural adjustments have been minimal, the Initiative's undertakings are well positioned for stimulating behavioural alterations in the long run. Its endeavours have been clear-cut, have shown high degrees of implementability, and have generally been well-received by target audiences.	The Initiative has delivered on its mandate to the extent that it has issued policy recommendations for enhancing international stability and security in cyberspace but has had limited success vis-à-vis effectively reducing the numbers of international cyberpolicy challenges, or achieving greater peace and civility in cyberspace, respectively.
Low	-	-	-

Table 6.6: Effectiveness Review: Carnegie Endowment Cyber Policy Initiative.

ideational commitments from governmental and non-governmental stakeholders, the Carnegie Cyber Policy Initiative has laid important foundations for thicker normative textures and unambiguous ideational accessions in the future.

6.4 Stakeholder-Cluster Synthesis: Encouraging Alignment

Following analyses related to the cybersecurity governance inputs of civil society and academia, as well as corporate actors, this chapter has explored the roles assumed by

three pertinent expert communities concerned with creating rules of the road for the virtual realm. Specifically, it has examined the cybersecurity norm creation activities of the *Global Commission on the Stability of Cyberspace (GCSC)*, the *Forum of Incident Response and Security Teams (FIRST)*, and *Carnegie Endowment for International Peace*. Similar to other policy areas, e.g. sustainable development, as well as the preceding case study analyses, cybersecurity norm development processes have profited from and been shaped markedly by expert proposals and views.

Thematic reviews of primary and secondary artefacts related to the three expert communities analysed have exposed that with regard to promoting norms of responsible behaviour in cyberspace, these actors have made important sensitising and substantive contributions. Covering an extensive spectrum of roles, they have chiefly acted as awareness raisers, and norm leaders as well as cooperation incubators.

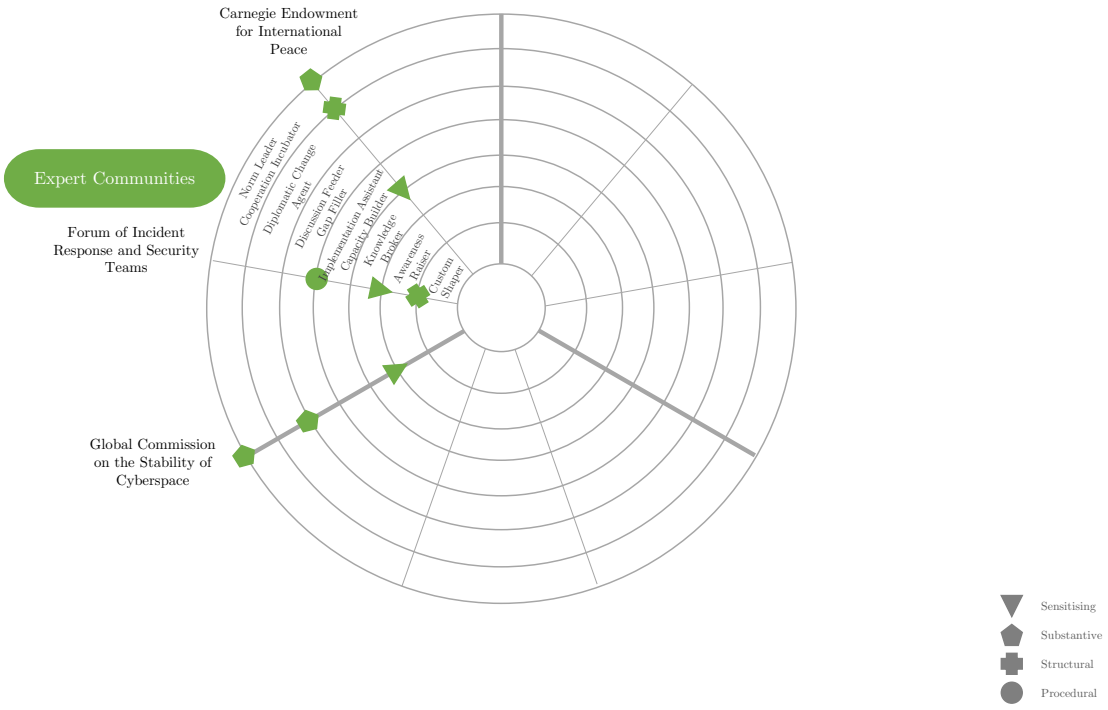

Figure 6.4: Expert Communities Contributions Spectrum.

Coming from different organisational origins and associations (a dedicated, externally-established commission of experts, a technically-oriented incident response organisation, as well as a foreign policy think tank), the three expert communities selected for analysis have advanced knowledge about rules of the road for cyberspace across technical and non-technical communities, and by so doing have stimulated cross-sectoral cooperation and collaboration.

Politically experienced and well connected expert communities, including the Global Commission on the Stability of Cyberspace, as well as Carnegie Endowment's Cyber Policy Initiative have crafted targeted ideational proposals and have brokered these strategically across leading policy mechanisms and high-ranking dialogue venues, including the United Nations, the G20, and the Munich Security Conference. Their activities have been far-reaching, and their normative proposals well-crafted to resonate with diverse target audiences. As per the expert interviews conducted, the alignment and exchange with leading policymakers and fora were deliberate strategic choices with a view to extending the reach and acceptance of the efforts proposed.[854] To a certain extent, these politically well-connected expert communities have taken on authoritative roles and regulatory functions previously ascribed to governmental entities, for instance, norm leadership, which is also why these entities have been attested high levels of output and outcome effectiveness. More technically-minded expert communities, such as FIRST have provided invaluable input in terms of kicking off processes of norms operationalisation, and building relevant capacities across technical and policy communities.[855]

In terms of broader systemic effects pertaining to their activities, expert communities have been faced with challenges similar to those confronting representatives from civil

[854] Interview #9 (n 445); Expert #1, Interview #1 (2019); Expert #17, Interview #17 (2019); Interview #32 (n 838).

[855] Interview #12 (n 810).

society and academia. Despite heightened levels of activities and normative stipulations made by the expert communities surveyed, offensive cyberoperations and attacks have not abated nor have the proposed norms seen far-reaching enforcement. Notwithstanding their so far limited ability to effect broader systemic changes, these actors have issued important building blocks for initiating next steps, e.g. operationalising the normative proposals issued and ensuring compliance with the corresponding stipulations.

The global policy arena is filled with a wide variety of actors – international organisations, corporations, professional associations, advocacy groups, and the like – seeking to govern activity in issue areas they care about. These actors are not merely occupying global structures. They are active agents who want new structures and rules (or different rules) to solve problems, change outcomes, and transform international life.

— Deborah D. Avant, Martha Finnemore and Susan K. Sell, *Who Governs the Globe? (2010)*

7

Implications and Challenges

Contents

7.1 Key Findings and Discussion

Pursuant to the case studies examined across *Chapters 4*, *5*, and *6*, this chapter summarises and discusses the main insights acquired, and dissects pertinent accountability and legitimacy questions resulting from non-state efforts centred around creating rules of the road for the virtual realm. In addition to highlighting key accountability challenges, the chapter also offers preliminary policy recommendations for achieving further progress vis-à-vis addressing these challenges and anchoring responsibilities for responsible behaviour in cyberspace. At a macro level, the examinations conducted have echoed research findings of broader studies of transnational governance. For instance, similar to what has been observed in studies concerned with transnational environmental

governance arrangements, the scientific and technical underpinnings relating to debates about norms of responsible behaviour in cyberspace have allowed private actors with expertise, including corporations, dedicated commissions and groupings, as well as academic and civil society representatives, to partake in governance activities.[856] Scholars, including Hale, for instance, have observed 'how multinational corporations can use their financial resources, market influence, and transboundary reach to establish themselves as *global governors*, and how NGOs possess moral authority that is often needed for transnational governance to be legitimate and credible'.[857]

From politico-legal/systemic-strategic perspectives, the broader international policy environment has not been very 'conducive to discussions of how best to coordinate responses to the complex, cross-border dilemmas emerging around new technologies'.[858] States have been caught up in lengthy multilateral deliberations and have failed to make meaningful progress on key questions, such as how international legal provisions apply to cyberspace. Against the background of increasing levels of uncertainty around key tenets of responsible behaviour in cyberspace, non-state actors have taken it upon themselves to contribute to and move forward global cybersecurity norm formation processes. Indeed, as has been demonstrated, actors from different stakeholder groups, including civil society and academia, corporate entities, as well as expert communities have been 'intent on shaping the science, morality and laws of new technologies ..., with limited public debate underpinning or guiding their efforts', particularly in the case of corporate actors.[859] Given the depth and breadth of their contributions, however, examining underlying accountability and legitimacy questions, as well as addressing

---

856 Thomas Hale, 'Transnational Actors and Transnational Governance in Global Environmental Politics' (2020) 23 Annual Review of Political Science 203 ⟨https://perma.cc/BV75-C4VL⟩.

857 Ibid 208.

858 Kavanagh, 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (n 699) 5.

859 Ibid 4.

issues related to limited public scrutiny are critical for rendering global cybersecurity norm formation processes more systemically effective and sustainable.

The case-level examinations have shown that non-state actors have come to yield considerable decisional, discursive, and regulatory power, that is to say they have influenced decision-making, discourses, and rule-making endeavours.[860] With reference to the thematic examinations conducted and the analytical tools developed in *Chapter 3*, non-state entities have been seen to act as (a) knowledge brokers, (b) awareness raisers, (c) norm leaders and cooperation incubators, (d) diplomatic change agents, (e) discussion feeders and gap fillers, (f) implementation assistants and capacity builders, and (g) custom shapers. In concurrence with the different parts executed, their contributions have displayed (a) sensitising, (b) substantive, (c) structural, as well as (d) procedural qualities.

Conceptually and analytically, the case study examinations have added to more fine-grained understandings of the different steering parts conducted by non-state actors. The roles of non-traditional security agents in the digital domain have frequently and unsuitably been reduced to advocacy and lobbying endeavours, and have generally remained under-theorised.[861] While advocacy-oriented efforts still figure on the spectrum of roles assumed, the results of the case study analyses have demonstrated that advocacy-centred efforts are but one type of non-state actor activity executed in the context of promoting peaceful interaction in cyberspace.

In seeking to provide an overview of how and with which qualities non-state actors have contributed to global cybersecurity norm formation processes, this thesis has developed a *non-state actor contributions spectrum* (please refer to Figure 7.1). The

---

860 The three faces of power can be distinguished as follows: Decisional power refers to actors' capacities to influence decision-making, discursive power to their potentials to (re)frame discourses, and regulatory power to their abilities to (re)make rules, see Arts (n 231).

861 Breslin and Nesadurai (n 44).

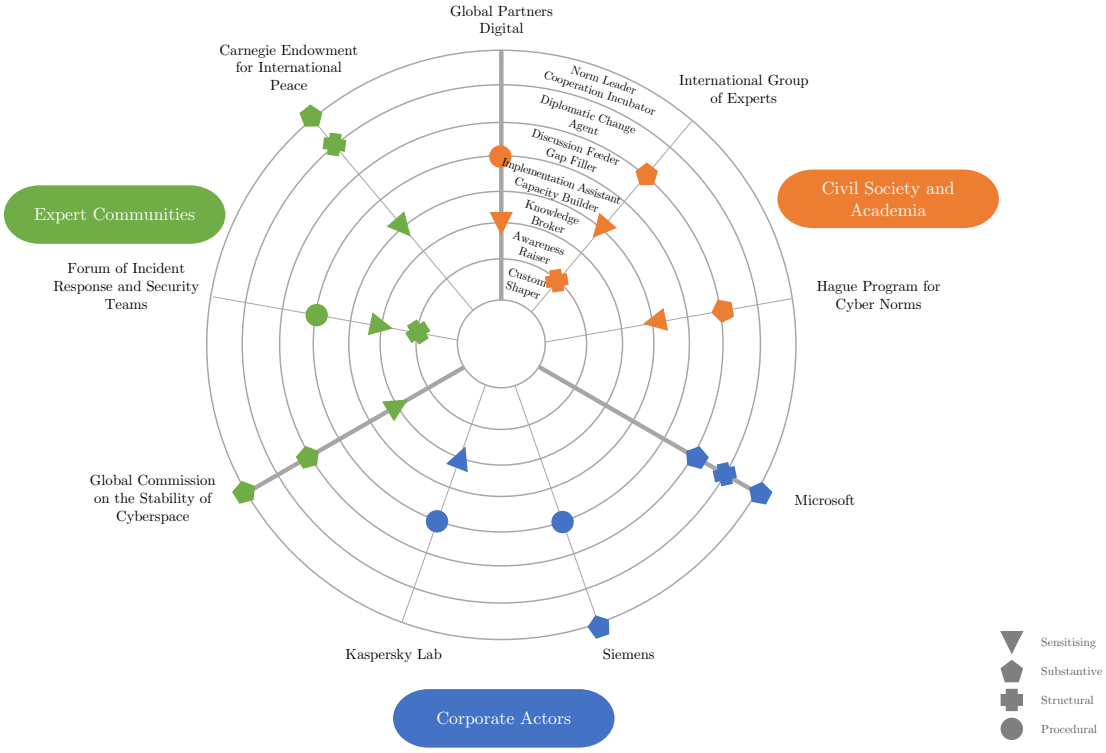

Figure 7.1: Non-State Actor Contributions Spectrum.

latter is a conceptual tool which helps plot the different parts assumed by non-state actors in global cybersecurity norm formation processes and determine the qualitative characteristics of their contributions. The contributions spectrum consists of nested concentric circles which reflect the different non-state actor roles identified as part of the thematic examinations executed. Across the circles extend nine beams which represent the different actors analysed. The roles executed by the entities examined are flagged with either one of four symbols, which indicate the qualitative characteristics of the relevant non-state actor contributions, i.e. (a) sensitising, (b) substantive, (c) structural, and (d) procedural. In addition to providing structures for organisation and clustering, the spectrum helps illuminate qualitative variations concerning the contributions made by non-state actors to discussions about rules of the road for the virtual realm.

In terns of influence exerted, the examinations conducted have shown that the majority of actors surveyed have displayed high levels of output effectiveness. Depending

on the relevant role profiles taken on, they have, at times simultaneously, increased awareness and conducted advocacy around normative issues, participated in and responded to intergovernmental meetings, released specific proposals and inspired legal positioning, or have actively brokered knowledge between different stakeholder constituencies (governmental and non-governmental).

Non-state actors such as FIRST, Global Partners Digital, or Kaspersky Lab have consciously analysed and entered into global decision-making processes pertaining to rules of the road for the digital domain. With the goal of shaping the boundaries of their operational environments and (political) contexts, they have launched new ventures which tie together their strategic preferences and broader (political) discussions about rules of the road for cyberspace. They have realised that in order to be able to affect global governance projects concerning responsible behaviour in the virtual realm, they 'need to intervene directly or indirectly, in the decision-making process[es] they want to influence', e.g. by means of feeding relevant knowledge or directly participating in relevant fora. The case studies have further demonstrated that in the remit of lining out the boundaries of responsible conduct in cyberspace, non-state actors and their proposals appear to have benefited from having relevant resources at their disposal, including issue-relevant knowledge or expertise, as well as access to policy-makers and venues.[862]

Through drafting, conceptualising, and promoting politically relevant and timely ideas, principles, and norms, most of the non-state actors surveyed as part of this thesis have come to *co-determine* or at least influence noticeably the postures and actions of states and other participants in the global arena, i.e. they have come to generate and exert discursive power.[863] Discursive power can be understood as the ability to structure and re-structure discourses, whereby discourses refer to more or less coherent and

[862] Arts (n 231).

[863] Ibid 23.

related groups of 'values, norms, ideas, concepts, buzzwords, testimonies, etc., produced, reproduced or transformed by [groups] of societal actors, to give meaning to a certain practice', or sets of practices.[864] Conceptualised in this manner, discursive contributions and engagements imply acts of interpretation-structuring. For instance, with regard to developing rules of the road for the virtual realm, non-state actors, by formulating new normative ideas or redefining existing concepts and frames of reference, have given meaning to events pertaining to the promotion of responsible conduct in cyberspace. They have done so for their own purposes, 'in order to give signification to the world around them, but ... also ... to position themselves in relation to others'.[865] Hence, their discursive contributions have effects at two levels – an ego-level, and an alter-level.

Drawing on the case studies conducted, non-state actors, such as Microsoft, the Hague Program for Cyber Norms, or Siemens have exerted discursive power in cybersecurity norm formation processes. That is, they have defined

> their political ideals and values (ideal society, causal and normative beliefs), [have defined] their norms for political behaviour (rights and obligations), [have defined] what really matters and what not (ideas, concepts, buzzwords) and [have defined] their political strategies in order to persuade others of the appropriateness of their own worldview.[866]

Having access to relevant political venues and media, submitting morally authoritative claims, and deliberately linking their proposals to dominant discourses, has helped these actors succeed at restructuring and reinvigorating debates about rules of the road for the digital domain. Drawing on their technical acumen and subject matter expertise, they have granted themselves the rights to speak about norms of responsible behaviour in cyberspace 'in moral terms' in public venues and with the intention of convincing larger parts of society about their normative standpoints.[867]

---

[864] Arts (n 231) 23.

[865] Ibid 23.

[866] Ibid 24-25.

[867] Ibid.

As the case studies have clearly demonstrated, even across formerly predominantly state-driven issue areas, such as international security and stability, non-state actors have come to propose constitutive as well as regulative standards. As Arts has fittingly recognised, non-state actors 'are no longer merely watching, influencing and waiting for governments and intergovernmental organisations to establish public rules on various matters'.[868] Instead, they actively seek to shape regulatory environments and carve out spaces for rules-oriented contributions. In the context of weighing in on global governance arrangements pertaining to the virtual realm, private protagonists, including Microsoft, Siemens, the Global Commission on the Stability of Cyberspace, as well as Carnegie Endowment for International Peace, the Hague Program for Cyber Norms and the second International Group of Experts have actively sought to fill institutional caveats with new stipulations to guide behaviours, and establish shared expectations of roles and agencies. The regulatory capabilities exerted by these non-state actors have led to 'new forms of authority structures' and sites of value allocation.[869]

The levels of norms-related engagement pursued by the non-state actors surveyed as part of the preceding chapters raise several important accountability challenges which will be discussed in greater detail below.

> Because state actors are absent or have minimal direct roles in [some of] these private voluntary regulatory schemes, they raise important questions about how these schemes emerge and are then adopted by those who choose to voluntarily commit to these standards in the absence of state directives to do so.[870]

As is evident from the breadth of roles assumed and the quality of contributions made (please refer to Figure 7.1), the efforts and proposals issued by these private entities have transpired beyond traditional frames of (state-centred) authority and have

---

868 Arts (n 231) 30.

869 Breslin and Nesadurai (n 44) 188.

870 Ibid 189.

come to involve and span across multiple levels – inter-industry, intergovernmental, and transnational levels.[871] The case studies analysed have clearly shown that private protagonists have taken on governing roles, which stretch far beyond engaging in advocacy or lobbying efforts. To illustrate, some of their proposals and ideational constructs have made it into policy documents of large multilateral institutions and multistakeholder venues, including the European Union, the Paris Peace Forum, or the UN Internet Governance Forum.

While having discharged forces of pluralisation, the cybersecurity norm formation endeavours launched by members of civil society and academia, industry heavyweights, and expert groups have also brought about further forces of norms-related fragmentation. Cybersecurity norm formation processes have grown in numbers as well as substantive elements, and have been shaped by different underlying interests and motivations. Citing Ruhl and others, fragmented processes are the results of 'different states or stakeholders preferring specific fora that they believe will most align with their interests'.[872] Furthermore, as Breslin and Nesadurai have aptly observed in the context of non-state actors and transnational governance in Southeast Asia, in multi-polar contexts 'states and non-state actors operate at times independently of each other, at times in open rivalry, and sometimes as cooperative partners in constructing new emergent structures of order'.[873] As the case studies have evidenced, these observations also hold true with regard to setting rules of the game for cyberspace, where non-state actors have at times been seen to work in alliance with state actors and at others independently of state entities.

Apart from scattered collections of of actors, fora, or proposals, fragmented processes can also refer to 'thin social linkages', weakening or even preventing more

---

871 Breslin and Nesadurai (n 44).

872 Ruhl and others (n 314) 13.

873 Breslin and Nesadurai (n 44) 198.

cohesive structures.[874]

> Under such conditions, transnational actors are more able to deploy such tactics as forum-shopping (trading between different options) and forum-linking (combining otherwise disparate issues or institutional processes) to suit their interests. Arguably, however, transnational linkages may help to bring some order to this pluralistic institutional setting by diffusing common norms and thickening relational ties.[875]

With reference to the above, situations of fragmentation can present relevant participants and processes with both opportunities and challenges (or advantages and disadvantages, respectively). For one thing, higher levels of fragmentation may increase the diversity of contributors as well as issues, and may yield greater chances for reflecting and integrating the opinions and viewpoints of broader categories of relevant actors. Furthermore, different endeavours may be initiated for different purposes and with different ambitions in mind, and using different venues. 'Norms may be more realistic in some areas than in others, such as peacetime use of cybercapabilities compared with military cyberoperations'.[876] Thus, pursuing multiple tracks can help preclude situations of total standstill and failure, and allow relevant other/parallel tracks to advance and achieve progress. Having a bouquet of different processes, i.e. industry-driven, civil-society-organised, expert-led, or multistakeholder-oriented processes, may on the one hand increase opportunities for complementarity and 'cross-pollination', and on the other hand strengthen levels of stakeholder-oriented relevance.[877] As Ruhl and others have maintained,

> fragmentation may be useful because different processes can address different stakeholders. Although multistakeholder efforts may also seek to use broad coalitions to endorse universal behaviour expectations, other cybernorm processes may be tailored to relevant communities. Hence,

---

874 Hale (n 856).

875 Ibid 212.

876 Ruhl and others (n 314) 13.

877 Ibid.

> certain cybernorm processes may appropriately focus on creating rules of the road for states while others may emphasise rules of the road for industry.[878]

Furthermore, fragmented processes can work in two directions. In line with what has been observed as part of the case study analyses, they can, for one thing, support procedural broadening, and for another contribute to substantive deepening. Efforts conducted by actors such as the Global Commission on the Stability of Cyberspace, the second International Group of Experts, or Carnegie Endowment's Cyber Policy Initiative, for instance, have centred on tightening substantive aspects pertaining to rules of the road for cyberspace, and have focused on elements of implementation and operationalisation. In contrast, the activities conducted by Microsoft, Siemens, or Kaspersky Lab have displayed greater attributes of procedural broadening, trying to convince as many different stakeholders as possible to support endeavours concerning the promotion of responsible behaviour in cyberspace.

While scattered process landscapes may foster advancement of different streams even in the face of politically or internationally adverse conditions (as has been the case in the context of promoting rules of the road for cyberspace), high levels of fragmentation related to norm formation processes can also present significant challenges. For one thing, there are no guarantees that higher levels of diversity and cross-pollination will eventually lead to consolidation and generate widely-shared rules of the road for cyberspace. Indeed, high levels of fragmentation can give rise to situations of greater uncertainty and process-trade-offs, or races to the bottom, leading to sub-optimal results and a watering-down or complete destruction of cybersecurity norm-building endeavours and normative commitments. Maintaining highly dispersed process landscapes over the long run may also be strategically or politically unsustainable and costly. 'Although fragmentation may be useful (or at least not a harm) at present and in the short

[878] Ruhl and others (n 314) 14.

term, ... process consolidation may be a necessary step if a truly universal set of global cybernorms is to develop'.[879]

Moreover, and more importantly, highly dispersed process landscapes like the ones observed as part of the analyses conducted often go hand in hand with far-reaching accountability issues (i.e. which actors are responsible for which processes/process elements), and contests over authority/legitimacy (i.e. which entities have legitimate claims or the right to determine the norms and rules that ought to be complied with).[880]

7.2 Legitimacy and Accountability Challenges

The case study examinations have evidenced that cybersecurity norms-oriented non-state actors, proposals, and fora have proliferated substantially over the past years, often in the shadows of, or 'with limited public debate underpinning or guiding their efforts'.[881] Given the extensive depth and breadth of their contributions, however, and because 'state actors are absent or have minimal direct roles in [some of] these private voluntary regulatory schemes', it is important to dissect underlying accountability and legitimacy questions pertaining to non-state actor-driven cybersecurity norm formation efforts (e.g. *how do these actors justify their activities*).

This thesis argues that the cybersecurity norms-related activities conducted by non-state actors raise at least three critical accountability challenges: (a) the problem of many hands, (b) the profusion of issue areas, (c) and the fluidity and malleability of institutional arrangements.[882] It further holds that these three challenges are the

[879] Ruhl and others (n 314).

[880] Breslin and Nesadurai (n 44).

[881] Kavanagh, 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (n 699) 4.

[882] Parts of this chapter have been published as Eggenschwiler, 'Accountability Challenges Confronting Cyberspace Governance' (n 96), and Eggenschwiler, *International Cybersecurity Norm Development: The Roles of States Post-2017* (n 216), respectively.

results of actor-, subject-, and venue-related elements of fragmentation. To illustrate, in the context of developing rules of the road for the digital realm, questions such as, *who is accountable to whom, for what, by which standards, and why*, cannot be answered easily, and are further confounded by non-state actors contributing to norm formation ventures.[883] Yet, in terms of realising systemic changes in conduct, achieving compliance, and ensuring norms-based enforcement, instituting mechanisms of answerability, and being able to determine relevant responsibilities (which may also lie with non-state actors) are critical aspects. Addressing questions pertaining to legitimacy and accountability is also important in light of the critical/sensitive nature of cybersecurity issues, as well as the types and scope of rule-making endeavours pursued by non-state actors, and the authoritative claims made, respectively.

Conceptually, accountability is confronted with similar definitional muddles as those introduced in *Chapter 2* in relation to cyberspace and cybersecurity. Accountability has become something of a catchword, and although scholars seem to agree on the concept's overall importance, they appear to be less unified apropos its constitutive elements. Consciously abstaining from advancing yet another definition or reinterpretation of the concept, and increasing the term's elusiveness further, this manuscript relies on what Bovens, Goodin and Schillemans have termed the minimal conceptual consensus.

> The minimal conceptual consensus entails, first of all, that accountability is about providing answers; is about answerability towards others with a legitimate claim to demand an account. Accountability is then a relational concept, linking those who owe an account and those to whom it is owed. Accountability is a relational concept in another sense as well, linking agents and others for whom they perform tasks or who are affected by the tasks they perform.[884]

---

883 Mark Bovens, Robert E Goodin, and Thomas Schillemans, 'Public Accountability' in Mark Bovens, Robert E Goodin, and Thomas Schillemans (eds), *The Oxford Handbook of Public Accountability* (Oxford University Press 2014) ⟨https://perma.cc/CMF8-UUBZ⟩.

884 Ibid 6.

In order to counter tendencies of disintegration and ensure continuous openness and stability of the digital environment, tangible accountability structures are of vital importance.[885] However, the three accountability challenges identified in the context of governing conduct in cyberspace profoundly compound basic answerability structures.

The first accountability challenge identified in the remit of private contributions to cybersecurity norm formation processes, i.e. the problem of many hands, refers to conditions of accountability obfuscation caused by large numbers of different actors engaged in concurring regulatory ventures.[886] 'Because many different officials contribute in many ways to decisions and policies ... it is difficult even in principle to identify who is morally responsible for political outcomes'.[887] As the previous chapters have evidenced, in the context of promoting rules of the road for cyberspace, entities contributing to policy outcomes and regulatory deliberations have grown immensely. While the large numbers of contributors involved in cyberspace governance do not necessarily imply an absence of accountability mechanisms, they do mean higher degrees of complexity. The heterogeneity of stakeholder configurations can aggravate questions pertaining to agency and influence. Accountability structures are more difficult to determine because actors co-produce outcomes and contribute to the end-product in hybrid constellations. With reference to the case studies carried out, instances of co-production have, among others, been observable in the context of the Paris Call for Trust and Security in Cyberspace and the UN OEWG. In these instances non-state actors have collaborated and co-produced outcomes with state actors but have not claimed or been awarded process ownership and accountability for specific results.

---

885 Jan Aart Scholte, *Building Global Democracy?* (Jan Aart Scholte ed, Cambridge University Press 2011).

886 Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13(4) European Law Journal 447 ⟨https://perma.cc/775V-AJQU⟩; Yannis Papadopoulos, 'Cooperative Forms of Governance: Problems of Democratic Accountability in Complex Environments' (2003) 42(4) European Journal of Political Research 473 ⟨https://perma.cc/R2FE-2GVP⟩.

887 Dennis F Thompson, 'Moral Responsibility of Public Officials: The Problem of Many Hands' (1980) 74(4) American Political Science Review 905 ⟨https://perma.cc/S9ND-RRQD⟩, 905.

Accountability structures can further be complicated by the conflation of stakeholder-specific traditions, standards, and expectations.[888] Not only are the types of actors contributing to governance ventures and their goals larger, making the identification of accountability objects more difficult (i.e. *for which goals should accountability be rendered and by whom*), but their expectations can diverge and complicate the emergence of clear lines of responsibility or accountability.[889] Indeed, environments characterised by multiple stakeholders tend to provide opportunities for blame-shifting and accountability evasion.[890] With regard to the challenges resulting from the many hands involved in transnational governance schemes, Black has usefully noted that

> it is hard to hold the standard setter to account for the ways in which the rules have been enforced – but potentially difficult to hold the enforcer to account for rules it did not write. Here the issue is not, or rather not simply, how to call to account a single organisation, but how to call to account a constellation of regulators. Is the appropriate course to identify one regulator and argue that the accountability of the others is derived from and dependent on the accountability of that regulator, as in hierarchical regimes (one for all)? Or is the appropriate course to say that each regulator has to be individually accountable for the activities of the regime as a whole (all for one)? Alternatively, should each actor be held accountable just for its own role within the regime (each for itself)?[891]

Viewed in the context of developing rules of the road for cyberspace, it remains unclear who carries accountability for the (successful) application and enforcement of norms – state actors or non-state actors, or both, and if the latter, how is accountability shared?

The profusion of issue areas which involve and reach across technical, socio-political, and economic spheres, constitutes another accountability conundrum. In terms of

---

888 Jonathan GS Koppell, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"' (2005) 65(1) Public Administration Review 94 ⟨https://perma.cc/Q86G-YVYS⟩.

889 Bovens, Goodin, and Schillemans (n 883); Carr (n 244).

890 Yannis Papadopoulos, 'Accountability and Multi-level Governance: More Accountability, Less Democracy?' (2010) 33(5) West European Politics 1030 ⟨https://perma.cc/DP8Q-8VXF⟩.

891 Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 143.

promoting responsible behaviour in cyberspace and ensuring compliance with the norms stipulated, the excess and coming together of technical and non-technical topics driven by different non-state actors convolute responsibility-related questions because operationalisation and enforcement processes may, for instance, occur at different levels, in alignment with relevant actor-based interpretations or proposals brought forward (e.g. technical implementation versus policy-oriented implementation). The confluence of issue areas can lead to 'tangled web[s] of relationships'.[892] Left unaddressed and tangled, these intertwined webs of relationships can have fatal consequences for accountability structures. For one thing, they can result in the erosion of (pre-existing) accountability structures and cause accountability deficits because clear accountability margins become increasingly blurred. For another thing, they can lead to dysfunctional amalgamations of accountability arrangements and bring about situations of accountability overcrowding.[893]

With reference to the experts interviewed for this thesis, few had clear answers for which (process)elements and stipulations (technical/non-technical), or whom the various norm-proposing non-state actors owe account to, other than the promotion of responsible behaviour in cyberspace generally, and the broader internet community, respectively. To provide another example pertaining to the profusion of issue areas, the stipulation to disclose not publicly known ICT vulnerabilities, for example, may appear to be a fairly-straight forward, technically/database-oriented process to be carried out by threat experts or dedicated observatories. However, depending on the types and modes of implementation, the operationalisation of this norm can bring about far-reaching policy and legal challenges on the parts of state/corporate entities and security researchers alike.

---

[892] Melvin J Dubnick and HGeorge Frederickson, *Accountable Governance* (Routledge 2014) ⟨https://perma.cc/GGK3-M8U3⟩ xxi.

[893] Bovens (n 886).

> Individuals who discover a vulnerability often face legal threats when they decide to report it. These threats can have implications on not only civil and criminal law but also contract law, licensing, patent law and other types of legislation. Discoverers may find themselves in a grey area due to the methods used to discover the vulnerability and the way it was disclosed.[894]

In the example cited, issue area-related conflations can lead to dysfunctional amalgamations of accountability arrangements/regimes.

The fluidity of processes and institutional arrangements relating to the promotion of responsible behaviour in the virtual realm poses yet another accountability problem. It has been established that most of the non-state actors surveyed as part of this thesis have started to pursue norms-related processes only a few years ago, and with regard to their means of engagement, activities, and tenure have displayed elements of fluidity/liquidity and ad hocism. In the case of corporate entities, for instance, shifting overarching strategic priorities may go hand in hand with changes in norms-related commitments and timelines. Furthermore, accountability structures tend to suffer from the dispersion of topics across different procedural and organisational settings and related institutional volatility. They are likely to be strained by the fact that stakeholders can take on different roles across different fora, and employ different venues for their purposes, i.e. conduct forum-shopping. Forum shopping refers to actor-based practices of deliberately choosing discussion sites with the highest assumed rates of success for their policy objectives. Among other things, forum-shopping tactics are employed to 'evade perceived unfavourable institutional characteristics' in some venues, and locate debates or generate discussions in other, ostensibly more amenable arenas.[895] Forum shopping schemes introduce elements of (strategic) inconsistency

---

[894] European Union Agency for Network and Information Security, *ENISA Good Practice Guide on Vulnerability Disclosure* (techspace rep, November, European Union Agency for Network and Information Security 2015) ⟨https://perma.cc/U5UR-ZYPJ⟩ 7.

[895] Hannah Murphy and Aynsley Kellow, 'Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas' (2013) 4(2) Global Policy 139 ⟨https://perma.cc/3E75-TD8G⟩, 145.

and make it difficult for accountability structures to take hold. What is more, the fluidity of institutional setups also makes developments hard to track and procedural access for some stakeholders, including civil society representatives, uneven, thereby undermining processes of public account giving.[896] In the context of promoting rules of the road for cyberspace, civil society organisations have repeatedly voiced concerns about unequal participation and the fact that decisions of sensitive, yet far-reaching nature are made behind closed doors across several UN-centred fora.

Environments determined by large numbers of non-state norm setters, or polycentric regulatory regimes, as found in the case of promoting norms of responsible behaviour in cyberspace, unsettle traditional authority and legitimacy structures. In settings, which are characterised by high levels of complexity, disintegration, and interdependence between stakeholders, 'in which state and non-state actors are both regulators and regulated, and their boundaries are marked by the issues or problems which they are concerned with, rather than necessarily by a common solution', traditional responsibility structures do not constitute common features.[897] On the contrary, in circumstances of this nature, social credibility and acceptability are often established on non-legal bases. Indeed, where governance arrangements are largely non-legal and where loci of authority are dispersed, applying legal conceptions of legitimacy may lead to incomplete understandings of these arrangements and may detract from other sources of social acceptability. Polycentric regulatory regimes may very well be seen as legitimate despite lacking formal legal authority.[898]

The next few paragraphs will look at how non-state actors participating in governance activities related to creating rules of the road for cyberspace have sought

---

[896] Sash Jayawardane, Joris Larik, and Erin Jackson, *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance* (techspace rep, The Hague Institute for Global Justice 2015) ⟨https://perma.cc/P9A6-RJ4X⟩.

[897] Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 143.

[898] Ibid.

to legitimise their endeavours, and have built their social credibility vis-à-vis different stakeholders.

Generally speaking, actors engaged in norm-setting or regulatory endeavours require legitimacy to bring their efforts to fruition and achieve behavioural alterations. Acquiring social credibility and acceptability is particularly relevant for non-state regulators as they cannot (or only rarely) fall back on governmental mandates or international legal accords for establishing their authority.[899] Definitionally, legitimacy refers to 'a generalised perception or assumption that the actions of [governing entities] are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions'.[900] According to Heywood, legitimacy is 'the quality that transforms naked power into rightful authority' and ensures voluntary (or quasi-voluntary) compliance with the stipulations issued by relevant governors.[901] To illustrate, in the context of developing norms of responsible behaviour in cyberspace, non-state actors depend on the perceptions and acceptability of those entities they aspire to govern, including fellow private actors, as well as states, which forces them to build up legitimacy on multiple fronts. For non-state actors engaged in cybersecurity norm-making endeavours, 'satisfying multiple legitimacy communities ... is particularly necessary if their authority is to be recognised and accepted, and thus for their continued survival' as entities with regulatory ambitions and functions.[902]

---

899 According to Black, 'non-state regulators cannot necessarily rely on the authority of law to motivate people to behave, or derive their legitimacy from their position in a wider legal order and constitutional settlement. They have to create the motivation for compliance or change in some other way', see Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 148.

900 Mark C Suchman, 'Managing Legitimacy: Strategic and Institutional Approaches' (1995) 20(3) The Academy of Management Review 571 ⟨https://perma.cc/A2CW-DMQR⟩, 574.

901 Andrew Heywood, *Political Theory: An Introduction* (Andrew Heywood ed, Palgrave Macmillan 2004) 141.

902 Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 149.

Because the activities of the non-state actors examined have neither been authorised by national or international bodies of law, linked to specific jurisdictional confines or accountability communities, nor instituted with options for recourse, they raise important legitimacy questions. Scholars studying transnational governance arrangements have argued that there is no guarantee that non-state actors engaging in global governance projects are able to represent relevant stakeholder voices equally and consistently and disregard particular (economic) interests, or that non-state endeavours yield higher problem-solving capabilities.

The case-level examinations have shown that rather than on formal democratic or legal mandates, the non-state actors surveyed have invoked (a) pragmatic, (b) moral, (c) cognitive, and (d) knowledge-based legitimacy frames for justifying their activities. Pragmatic legitimacy appeals revolve around the interests of relevant social groups. Non-state actors seeking to stipulate rules of the road for the virtual realm look to acquire social credibility for their activities by aligning the latter with the interests of the relevant social groups they intend to convince, either directly or indirectly. Moral strategies for gaining legitimacy place special emphasis on connecting to existing social values and principles held by relevant audiences, so the activities of norm proposers are considered morally appropriate. Cognitive legitimacy approaches on the other hand portray cybersecurity norm-making endeavours by non-state actors as given or necessary, e.g. by virtue of the size of their operations or systemic relevance, and knowledge-based legitimacy schemes endeavour to achieve broad levels of acceptability on the bases of proven know-how and subject matter expertise.[903]

In line with the different roles executed by the non-state actors surveyed across *Chapters 4*, *5*, and *6* and the correlating underlying qualities of their activities (i.e. (a) sensitising, (b) substantive, (c) structural, and (d) procedural), as well as their

[903] Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43).

respective areas of know-how, legitimacy frames have varied. For example, as technically-oriented, trust-based consortium of incident response teams, FIRST has relied on scientific/knowledge-based legitimacy frames to justify its contributions to cybersecurity norm formation processes. The contextual proximity between FIRST's norm-promoting activities and its core areas of expertise, as well as the organisation's ability to transfer and apply knowledge from technical to policy environments have allowed it to be viewed, by members of both technical and policy communities, as legitimate and relevant actor adding value to debates about responsible behaviour in cyberspace.[904]

In contrast, economically strong and internationally well-embedded actors such as Siemens or Microsoft have primarily employed pragmatic and cognitive legitimacy frames. Using their respective market powers, both actors have actively pursued alliances with like-minded political entities, including the Munich Security Conference in the case of Siemens, or the French Government in the case of Microsoft. With a view to attaining social credibility for their normative undertakings, these actors have sought to appeal to and reflect the interests of as many diverse stakeholder groups as possible. Employing arguments of size as well as capability and aligning them with dominant (Western) discourses, these corporations have succeeded at obtaining large numbers of signatures and credibility endorsements from fellow industry partners and stakeholders of other communities, including academia, and non-governmental organisations.

Social purpose corporations and academic institutions, on the other hand, including for instance Global Partners Digital or the Hague Program for Cyber Norms, have primarily used moral as well as knowledge-based strategies to legitimise their contributions to discussions about rules of the road for the virtual realm. As Florini has remarked in the context of human rights-promoting civil society organisations,

---

[904] Interview #28 (n 787); Interview #12 (n 810).

> the influence of transnational civil society ... stems from the power of moral authority and legitimacy, on the one hand, and the accepted claim to authoritative knowledge, on the other. These two aspects – moral authority and knowledge – go together and cannot be separated. Moral authority is directly related to the claim by transnational civil society that it somehow represents the *public interest* or the *common good* rather than private interests. INGOs can quickly lose their credibility if they become identified with some special economic or political interests.[905]

The civil society-related case studies surveyed in *Chapter 4* have revealed comparable learnings. The roles these actors have taken on in the remit of promoting responsible behaviour in cyberspace, i.e. knowledge brokers, awareness raisers, implementation assistants/capacity builders, and discussion feeders, have centred around and relied on references to subject-matter expertise and understanding, which in turn have been used as justificatory arguments for their proposals and commitments.

The different approaches to acquire social acceptability and credibility pursued by the non-state actors surveyed imply that legitimacy is conditioned as much by 'the values, interests, expectations, and cognitive frames' of those entities who are supportive of the relevant governance structures as it is by the structures themselves.[906]

> As such, legitimacy can differ significantly across time and space, and between actors, systems, and contexts. Although legitimacy claims may change, legitimacy can nonetheless be resilient – legitimacy communities may forgive individual transgressions, though the resilience of legitimacy may be linked to its basis: pragmatic legitimacy is less resilient than moral or normative legitimacy, which is in turn less resilient than cognitive legitimacy.[907]

Although analytically distinct concepts, legitimacy and accountability share close ties. Indeed, accountability structures are important baseline features for legitimacy

---

[905] Florini, *The Third Force: The Rise of Transnational Civil Society* (n 362) 186.

[906] Black, ''Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes' (n 43) 293.

[907] Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 145.

communities to formulate and submit their legitimacy claims to, and ensure they are valid and met by relevant governing entities. Through accountability structures, these communities look to assess the alignment with or discrepancy between their expectations of how these governance entities should operate, and their legitimacy claims voiced.[908]

7.3 Analytical Synthesis and Recommendations

Addressing the accountability- and legitimacy-related tensions identified, and tackling some of the corresponding concerns are tricky undertakings. However, thinking about and ideating potential solutions or devising relevant policy strategies are important aspects for moving accountability-oriented discussions forward (or indeed inciting discussions) and offering conceptual starting points for further progress. As has been noted, the vast scale and scope of global cybersecurity governance arrangements have rendered compliance and monitoring activities difficult. 'Without stronger monitoring frameworks, actors may be able to announce pledges with little fear of reputational consequences should they break them'.[909]

In line with Black, 'the search is on to find ways in which [polycentric regulatory regimes] can be enhanced' vis-à-vis attaining higher levels of accountability and legitimacy.[910] The succeeding paragraphs seek to respond to this quest. Specifically, they offer recommendations geared towards addressing the challenges introduced above and highlight avenues for generating accountable governance setups which take into account the high levels of fragmentation confronting cybersecurity norm formation ventures.

---

908 Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 149.

909 Hale (n 856) 213.

910 Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 137.

Cybersecurity norm promotion efforts have been seen to be 'institutionally diffuse and lack a single locus of supreme, absolute, and comprehensive authority'.[911] Given the degrees of diffusion as well as the absence of a final arbiter, accountability prescriptions centring on hierarchical command and control mechanisms appear ill-suited to resolve the tensions identified. Rather, accountability structures should be reflective of the diversity of stakeholders present in these debates, and be established on collective bases. The implementation of shared accountability structures may entail a deliberate rehashing of account rendering functions and processes. While the call for collective accountability structures does not imply the participation of the entirety of stakeholders, it does mean the enfranchisement of all relevant parties.[912] The enlistment of stakeholders essential to the resolution of specific cybersecurity governance problems, including among others corporate actors, representatives of civil society and expert groupings, presents an important first step with regard to streamlining collective accountability structures and identifying corresponding responsibilities.

In terms of realising dependable accountability structures, the institutionalisation of multistakeholder-oriented checks and balances is key. Independent, constitutionally inspired oversight mechanisms, such as ombudsmen or multistakeholder-versed third-party supervisory and review boards, and clear evaluation standards may provide useful starting points in this regard. The latter support the introduction of meaningful benchmarks of expected behaviour and set criteria against which conduct can be assessed transparently.[913] Given the heterogeneity of stakeholders, relevant standards need to be flexible, yet specific enough to take effect in the respective cybersecurity norm formation arenas.

---

911 Scholte, *Building Global Democracy?* (n 885) 18.

912 Jeremy Malcolm, 'Criteria of Meaningful Stakeholder Inclusion in Internet Governance' (2015) 4(4) Internet Policy Review ⟨https://perma.cc/56TW-HNGQ⟩.

913 Rolf H Weber, 'Accountabililty in Internet Governance' (2009) 13 International Journal of Communications Law and Policy 152 ⟨https://perma.cc/SW88-9FAG⟩.

Communities of practise focusing on specific cybersecurity norms-related issues may be useful tools with regard to institutionalising more flexible accountability structures. These communities assemble parties with vested interests in specific norms-based issue areas, and take into account the relevant contexts of interested parties. Entities with expertise related to specific proposals engage in dedicated development and implementation efforts. For example, 'the internet community [(e.g. ICANN or IETF)] could help advance, implement, and monitor the [GCSC's] proposed norm on protecting the public core of the internet, and developers may be most interested in the norm involving product tampering'.[914] Because these groups gather like-minded partners, and are smaller in scope and size than other cybersecurity norm venues, such as the UN IGF, for instance, accountability structures are likely to emerge quicker and with greater alignment. Given that these groups are structured around collaboration, expertise, and common interests, relevant group members may be inclined to take on accountability functions for specific deliverables more readily and voluntarily. As a result of the smaller numbers of actors and topics discussed in these communities, transparency concerns are also likely to improve as actors commit to dedicated and topically-bound deliverables. In addition, communities of practice enjoy considerable organisational freedom which would allow them to appoint oversight and recourse mechanisms, e.g. in the form of formally independent ombudsmen, as suggested above. Appointed ombudsmen could evaluate procedural complaints logged by community members, and promote understanding of pertinent community issues. 'Since governments, the private sector, the technical community, academia, and civil society are not monolithic entities', devising options which introduce norms-related accountability structures across diverse stakeholder communities (i.e. in the form of communities of practice), and have the potential to create complementarity among different norms proposals is critical, and

[914] Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492) 25.

provides means for fostering trust among norm-proposing entities.[915] Community-centred accountability approaches also help re-establish and anchor elements of agency and, by extension, responsibility.

With regard to the profusion of issue areas, the intertwining of political, technical, economic, and cultural dimensions, implies a conscious re-calibration of cybersecurity norms debates. Given the scale and scope of debates about rules of the road for the virtual realm, as well as ideological differences, introducing treaty mechanisms based on broadly framed policy/legal commitments, e.g. global calls, does not seem expedient. Rather, with reference to communities of practice, accountability discussions should be organised around specific, manageable issue areas, and include stakeholders from different backgrounds, which are capable of flagging areas of intersection and convergence. The identification of relevant issue areas around which procedures and actor expectations can converge is critical for the emergence of tangible accountability structures.[916] Issue specificity helps reduce ambiguity apropos actor relations, incentives, and goals, and allows for the strategic construction and connection of different aspects and elements of cybersecurity norms debates, as well as for the attribution of stakeholder responsibilities.[917]

In line with devoting more attention to issue-specificity, accountability-related complexities stemming from interconnected cybersecurity norms issues may be alleviated or structured more comprehensibly with help of relevant databases. Establishing transparent reference points along the lines of internationally shared archives of leading cybersecurity norms processes, their sponsors, initiators, addresses, key contents, goals, commitments, and anticipated timelines may reveal areas of issue-oriented

---

915 Global Commission on the Stability of Cyberspace, *Advancing Cyberstability* (n 492) 25.

916 Stephen D Krasner, *International Regimes* (Cornell University Press 1983).

917 Chelsey Slack, 'Wired Yet Disconnected: The Governance of International Cyber Relations' (2016) 7(1) Global Policy 69 ⟨https://perma.cc/N882-S5QJ⟩.

complementarity on the bases of which stakeholder assemblages can come together and interact. The *Cyber Norms Index* established by Carnegie Endowment's Cyber Policy Initiative has provided an early, yet incomplete, example in this regard.[918] In addition to anchoring responsibilities by transparently displaying information concerning initiators, etc., setting up and regularly feeding norms-related indices 'could also reflect how each process' work is received in other processes (that is, what sort of cross-pollination is occurring, or instances triggering competing or conflicting norms)'.[919] In the absence of clearly defined measures of account rendering pertaining to cybersecurity norm formation endeavours, globally accessible databases can offer useful correctives and important primers for more coherent and robust issue-based accountability structures.

Addressing and effectively tackling forum-related accountability challenges is just as exigent as dealing with actor- and issue-related problems. Venues discussing rules of the road for cyberspace have displayed high levels of transitoriness, i.e. they have been seen to emerge, vanish, and/or re-surface at times. According to Kusters and others, high transaction costs related to engaging in multistakeholder settings have led to 'processes of *muddling through*', murky accountability structures, and waning commitments on the parts of initial supporters.[920] Clearly specified, venue-related mission statements, and openly communicated roles could be important first steps for assigning responsibilities concerning the propagation of responsible conduct in the virtual realm across various fora.[921] Well-defined mission statements and mandates can help create longer-term allegiances and guidance, and reduce the risk of ad hocism and agenda shifting brought about by changing stakeholder configurations.

---

[918] Cyber Norms Index (n 825).

[919] Ruhl and others (n 314) 18.

[920] Koen Kusters and others, 'Participatory Planning, Monitoring and Evaluation of Multi-Stakeholder Platforms in Integrated Landscape Initiatives' (2018) 62(1) Environmental Management 170 ⟨https://perma.cc/Z3XT-GUHF⟩, 171.

[921] Malcolm (n 912).

Given that the survival rates of norms-oriented discussion sites are often determined by and contingent upon financial, and institutional promises voiced by state and non-state actors, crafting and introducing elements supporting clarity and longer-term orientation appear particularly important. Having clear understandings of the different roles of participating actors across different venues can support the emergence of distinguishable responsibility pockets. For instance, with regard to protecting the public core of the internet, more technically oriented actors including developers or DNS providers could assume dedicated responsibilities for laying out how to safeguard critical infrastructures, e.g. by means of implementing elevated security protocols, across venues such as the Paris Call for Trust and Security in Cyberspace. These commitments could help link discussions to specific fora, thereby creating path dependencies and baselines for emerging responsibility configurations. First attempts at pursuing strategies of this nature have been launched by the Hague Centre for Strategic Studies. The latter has committed to summoning a group of interested actors around protecting the public core of the internet. Under the umbrella of the Paris Call Principles, this assemblage of dedicated stakeholders is intended to

> examine the need to further refine the concept, discuss propagation, and explore options for implementation and monitoring of the principle as well as related norms. It will convene key stakeholders to raise awareness of the threats against the core internet protocols and functions, develop best practices and policy proposals for adoption and implementation, and advance common understandings of violations of the principle.[922]

By so doing, the Hague Centre for Strategic Studies has effectively created a nexus between discussions concerning the safeguarding of the public core of the internet and the Paris Call as appropriate venue for such discussions, thereby supporting the longer-term outlook of the forum as well. In order to address possible risks of these configurations and platforms resulting in talking clubs with no or little effects, being

[922] Paris Call for Trust and Security in Cyberspace (n 492).

clear and realistic about intended goals and defining executable, and clearly timed plans of action are critical elements to ensure.

With reference to institutional nontransparency, inaccessibility, and discrimination, structurally open and inclusive configurations can help bring about more accessible and tangible constructs of public account giving. Among other things, possibilities of defection and exclusion can be addressed by means of proactively disseminating 'pertinent, appropriate and quality information ... at the right time, in the right format, and through the right channels' to stakeholders that are significantly affected by specific policy problems or interested in the deliberation and resolution of cybersecurity governance issues, and providing avenues for raising concerns about certain institutions' undertakings and results.[923] Measures of this nature, simple though they may seem, can help create organisational openness and certainty, and foster continuous stakeholder buy-in. In addition, they serve as important stepping stones for more cohesive accountability measures, including independent audits or reviews, or other monitoring and control activities which can be executed on the bases of transparently communicated institutional settings and goals. Some of the non-governmental venues created in recent years, including the Global Commission on the Stability of Cyberspace, have been seen to pursue more accountable institutional strategies and have opened lines of communication and procedural access.

While it is key to address and strengthen accountability structures pertaining to cybersecurity norm formation processes, it is also important to acknowledge that, in light of the systemic factors which shape debates about responsible behaviour in cyberspace, authority structures are likely to remain essentially liquid, i.e. grounded

[923] World Health Organisation, *WHO Accountability Framework* (techspace rep, March, World Health Organisation 2015) ⟨https://perma.cc/7FV4-Y3T8⟩ 10.

in social relations rather than binding legal commitments.[924] As has become evident as part of this thesis, and has been aptly observed by Black,

> authority in the transnational context is informal, based on social and political acceptance not formal legal rules; it is ideational, based on ideas of what is the appropriate thing to do (though often articulated in technocratic terms and based on epistemic claims to expert knowledge); it is necessarily exercised through non-legal or *soft*law norms and *enforced* through social or community practices. Whilst authority can be based on a cognitive acceptance that a particular actor or group of actors are those who are most appropriate to govern, very often it is contested.[925]

Consequently, while accountability and legitimacy structures may crystallise, in the near-term, they are likely to 'remain brittle and vulnerable to challenge'.[926]

The expert voices consulted as part of this thesis have corroborated the fragility of and challenges pertaining to establishing responsibilities for transnational cybersecurity norm formation ventures. Interviewees representing corporate actors, for instance, have flagged their shareholders as primary accountees, and have only sporadically referenced other internet communities as accountability subjects.[927] Indeed, one interviewee has maintained that

> even as we sort of stumble into figuring out what the boundaries of this new ecosystem are, and ... what playing our respective roles looks like, it is clear that there are still respective roles. Stakeholder groups are still stakeholder groups and they have specific responsibilities. And there is also ... places in which we cannot, and we would not pretend to tell somebody else how to sort of think about these challenges. Governments have a unique responsibility to national security and for national defence that private companies do not. You know, we do not have a constituency or a population ... that we are accountable to in the way that governments are. And we do not have those same security responsibilities. So, there are ways in which the unique role of states and then the role of companies and

---

924 Black, ''Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes' (n 43).

925 Ibid 287.

926 Ibid 307.

927 Interview #21 (n 637); Expert #25, Interview #25 (2019); Interview #3 (n 533).

> civil society are still what they are. And there is limits to what they can do within those particular roles. And at the same time, I think we are also pushing ahead into a new world in which we need to rely on one another quite a bit more.[928]

Similarly, membership organisations have named their respective constituencies as primary accountability subjects but have at the same time also referenced wider internet communities as possible entities with legitimate claims for answers.[929] Comments on how accountability is to be rendered to those broader constituencies, however, have remained elusive.

Notions of fluidity and fragility have also transpired to legitimacy-related contexts. Despite the need and measures taken by the non-state entities surveyed to gain public credibility for their activities, none of the actors studied has defined clear indicators for assessing the effectiveness and uptake of their ventures. Though numbers of proposals and corresponding activities have increased considerably since 2017, effectiveness has not been assessed strategically. In terms of moving discussions forward and creating higher levels of answerability, however, it is imperative to know what works and what does not, especially also with a view to determining where to allocate hard incentives and resources to support norms implementation efforts. As Ruhl and others have suitably noted, the dictum

> *to measure is to know* may be applied in cyberspace. Objective, data-driven social science research [, for instance,] can help identify which norms already work and where diffusion is needed on others. Do states and other stakeholders operate consistent with the Global Commission's call to protect the public core of the internet? How often do states appear to *conduct or knowingly support* cyberoperations that *damage* or *other wise impair the use* of critical infrastructure contrary to the 2015 GGE norm that purports to prohibit such behaviour?[930]

---

928 Interview #11 (n 691).

929 Interview #27 (n 788); Expert #18, Interview #18 (2019); The Operationalization of Norms and Principles on Cybersecurity (n 723); Expert #16, Interview #16 (2019).

930 Ruhl and others (n 314) 17.

In addition to scientific research efforts, norm-proposing entities themselves would be well-advised to devise parameters along which to assess levels of goal attainment as well as uptake and enforcement of their proposals. More rigorously obtained and assessed data in turn could help solidify their bases of legitimacy vis-à-vis engaging in global regulatory projects pertaining to cyberspace (that is, if the data point to positive effects).

Where *hard* (measurable) metrics are difficult to devise or inadequate (e.g. given softer political and process-oriented contexts), simple effectiveness-oriented models such as those applied as part of this thesis (three-tier effectiveness review) or proposed by Ruhl and others (tracing cross-pollination), would already provide important yardsticks for assessing progress, or highlighting needs for strategic adjustments.[931] With regard to estimating ideational success, one of the experts interviewed, has held that

> I think the only real way to measure effectiveness is to see to what degree their [(norm-proposing non-state actors)] ideas are picked up and echoed by others. And what I mean with that is that, for instance, when we see the idea of the public core being incorporated in statements by governments that hold a lot more normative or even almost soft legal value, I think that is an indication that they are doing something valuable. ... Because these commitments are not just demands from governments, they typically are commitments on what the organisations themselves can do to make the internet a more peaceful and more reliable, more resilient place. So getting them to share the implementations that they have made, can help lead to those implementations echoing as best practice across the industry. And in many ways, I expect that is actually the outcome that we want to see. We want to see norms called out not just to have outreach when something happens, but to have some level of activity that makes the internet more resilient regardless of how people pick up on the specific norm or not. ... So I think we can measure it by seeing how much does an idea get picked up and gets echoed by multiple organisations, but also by how many best practices are we actually seeing shared and echoed within the community and implemented.[932]

More data-grounded understandings of how non-state-actor-driven cybersecurity norm formation endeavours effect changes or contribute to systemic improvements would

---

[931] Ruhl and others (n 314).

[932] Interview #12 (n 810).

help strengthen accountability and legitimacy structures, and solidify the responsibilities and authority of non-state actors in the virtual realm, respectively. Having clearer pictures of what works and what does not would also support moves towards greater consolidation and adoption. In keeping with Ruhl and others, while scattered norm formation processes may yield procedural benefits in the short to medium-term, more streamlined ventures would yield even greater substantive benefits in the long-term. 'Overlapping functions mean that multiple processes may be inefficient. Thinly stretched personnel and resources might be able to accomplish more with fewer processes (not to mention meetings)'.[933] Higher levels of consolidation and, by extension, cooperation could also accelerate diffusion and adoption speeds, as well as the implementation of sanctions regimes addressing non-conformity with cybersecurity norms.

Although discussions about rules of the road for the digital domain have been held since the late 1990s, diffusion and enforcement issues have not been addressed or tackled extensively and strategically by relevant norm-proposing stakeholders, recent spikes in levels of attention notwithstanding. The non-state actors analysed as part of this thesis, would be well-advised to move forward and support concrete enforcement proposals pertaining to their normative stipulations with a view to legitimising their normative ventures further. One of the experts interviewed has offered views on how enforcement of one of the norms advanced by the Global Commission on the Stability of Cyberspace could be promoted. Specifically, with reference to protecting the public core of the internet, Expert #12 has suggested that

> ... attacking the public core is actually quite expensive, because everyone uses it. So, everyone has some benefit of protecting it, and everyone can invest in, for instance, doing security testing on the software that makes up the public core. Now, let us say that states, for instance, committed that they will each invest a specific amount of money in, for instance, a bug bounty [programme] on any software that is part of the public core of the internet. That money could be used to harden the internet core, or

[933] Ruhl and others (n 314) 18.

> the public core, so significantly, that it would become more and more and more and more expensive for a state to actually violate the norm and go and attack the public core. And that actually drives them to a point where any attack they are going to do is going to be very limited, very restricted because they know that the price of upgrading their attack after people learn about it and defend against it, is going to be prohibitively expensive. So, I think for some of these norms, we can think about how we can put in place protocols, how we can put in place specific funding sources from the different states that agree to the norm to make them violating the norm almost too expensive to conduct. And I think those are going to be very, very important steps that we can take as a community to actually make these norms have teeth.[934]

What is more, enforcement-related questions represent wicked problems and are often accompanied and further confounded by attribution-related problems. Despite steadily improving SIGINT (signals intelligence) capabilities and forensics, identifying the perpetrators of malicious cyberactivities and ascribing blame for nefarious behaviour in the virtual realm beyond reasonable doubt have remained extremely difficult and contested undertakings. Yet, for cybersecurity norms to increase the levels of security and meet the high expectations attached to them, having clear understandings of who contravened which norms, to what degree of certainty, and with which consequences, is critical. However, '[t]he novel characteristics and complexities of cyberspace create significant hurdles for effective norms'.[935] Rather than with non-state actors, many experts interviewed have argued that enforcement activities primarily sit with states, given they enjoy international legal personality. Expert #3, for instance, has argued that

> enforcement is very difficult to share. We are ... very positive about, for instance, the new [EU] cybersanctions framework that came out in May [of 2019], that there will be more teeth for governments to do something. This particular framework does not necessarily guarantee the EU will impose sanctions for cyberattacks. [However,] it offers an opportunity. So, it is a first step. Having been in Council when this was just a glimmering idea years ago, I am very pleased to see that progress happened in Council as well. ... [Furthermore,] there have to be consequences for those who do not

---

934 Interview #12 (n 810).

935 Ruhl and others (n 314) 19.

> respect responsibility in cyberspace. And at this point, the only options are, you know, diplomatic measures, [i.e.] the various measures that are described in the cybertoolbox by the EU. Or even offensive cyberattacks as well. But that is really the last resort, I would say.[936]

Echoing these remarks, and applying them to the Global Commission on the Stability of Cyberspace, Expert #1 has maintained that

> ... the Commission does not do any enforcement, it does not have any power for enforcement. The Commission basically gives good advice and we believe that the advice is stronger because multiple stakeholders have been involved in the process, or at least the perspective of different stakeholders [has been] taken into account. That makes the advice stronger and better enforceable. Obviously, we do not have the power of economic sanctions. So, if you talk about enforcement, it is not – unfortunately it is never – multistakeholder.[937]

Adding qualifying notes, Expert #1 went on to state that '[a]lthough, if people pollute the public core, then if you look at the routing system, for instance, ... there are 60,000 actors. If people do wrong, they might be excluded from the routing system just by collective action'.[938]

Not only are these remarks emblematic of the fluid accountability and authority structures relating to discussions about responsible behaviour in cyberspace, they also underscore that the breadth and depth of normative conformity and enforcement are subject to debate and further evaluation.

7.4 Summary

Against the background of the case studies conducted across *Chapters 4*, *5*, and *6*, this chapter has underscored and commented on the levels of fragmentation evident

---

936 Interview #3 (n 533).

937 Interview #1 (n 854).

938 Ibid.

in debates about rules of the road for the virtual realm. Fragmented processes, it has been argued, can have both positive and negative aspects. For one thing, dispersed norm creation efforts driven by non-state actors have the potential to foster diversity and inclusion of voices from the periphery. Conversely though, scattered norm formation processes raise several critical accountability and legitimacy questions – who is accountable to whom, for what, by which standards, and why? With regard to promoting responsible behaviour in the virtual realm, this chapter has identified three key accountability problems resulting from non-state actor activities: (a) the problem of many hands, (b) the profusion of issue areas, (c) and the fluidity and malleability of institutional arrangements. These three challenges, it has been contended, are the results of actor-, subject-, and venue-related elements of fragmentation, and are characteristic for, or even constitutive of polycentric regulatory regimes. Structurally complex, polycentric regulatory regimes are at odds with traditional accountability and legitimacy constructs. This has been confirmed by the case studies conducted. Rather than on the bases of formal democratic or legal mandates, the non-state actors examined as part of the previous chapters have sought to actively manage and build their authority on the bases of pragmatic, moral, cognitive, and knowledge-based legitimacy frames.

With respect to addressing the challenges identified, this chapter has reasoned that in accordance with the distributed nature of the virtual realm, multistakeholder-oriented oversight mechanisms, as well as clear evaluation standards, and community-based responsibility anchors may provide useful starting points for inciting dependable accountability structures. Given the polycentric nature of debates about rules of the road for cyberspace, one-dimensional, sovereigntist accountability conceptions which intend to attach ultimate responsibility to a unitary source of authority seem misplaced. Accountability arrangements would benefit from consciously executed re-framing processes, involving all relevant stakeholders. 'All nodes in a given public policy network – including the global regulatory institutions involved – must play their part

in delivering transparency, consultation, evaluation and correction'.[939] Furthermore, accountability constructs would benefit from higher levels of issue specificity. Greater issue specificity would reduce ambiguity apropos actor relations, incentives, and goals, and would allow for the strategic construction and connection of different aspects and elements of cybersecurity norms debates, as well as for the attribution of stakeholder responsibilities.[940] Finally, with reference to tackling institutional transitoriness, clearly specified, venue-related mission statements, and openly communicated roles could be important first steps for establishing answerability provisions concerning the propagation of responsible conduct in the virtual realm across different fora.[941]

While it is possible for accountability and legitimacy structures to crystallise even in environments as complex and fragmented as those pertaining to norms of responsible behaviour in cyberspace, in the near-term, they are likely to remain fluid, open to contestation, and further unsettling. While fragmented cybersecurity norms processes do not necessarily imply negative consequences, in the medium to long term, they would benefit from greater alignment and consolidation (while still paying due regard to different voices raised in their creation). As Ruhl and others have noted, the different cybersecurity norms processes launched by non-state actors could be usefully linked 'if actors take seriously the reputational costs of being outside a cybernorm club'.[942]

In any case, what appears evident from the remarks above is that new, non-state actor-driven

> policy and regulatory approaches will require greater investment in transparency, oversight, and accountability mechanisms. ... This task should also entail ensuring that technology companies and organisations accept greater scrutiny. For example, tech companies should heighten internal

---

939 Scholte, *Building Global Democracy?* (n 885) 20.

940 Slack, 'Wired Yet Disconnected: The Governance of International Cyber Relations' (n 917).

941 Malcolm (n 912).

942 Ruhl and others (n 314) 15.

> monitoring and external reporting of their self-regulatory initiatives, provide appropriately insulated, publicly funded researchers with safe access to their data, and, above all, ensure that accountability covers all aspects of the supply chain and that both the direct and indirect costs (such as labour and environmental costs) of the technologies in question are clearly understood.[943]

And even though larger systemic conditions do not appear to be very conducive to the pursuit of shared normative ambitions and goals – as many governments follow isolationist and competitive strategies, and some corporate actors practise quasi-monopolies –, '[m]ore meaningful dialogue and cooperation – however difficult – on how technological developments are affecting societies and the uses and applications of technology generating the most disruption and contestation are urgently required'.[944] Among other things, higher levels of collaboration, especially in polycentric setups, can increase levels of legitimacy pertaining to non-state actor-driven governance ventures.

Going forward, and with reference to what has been seen following the collapse of the 2016-2017 UN GGE, it is likely that transnational governance setups will complement (or even substitute) state-based forms of steering in the context of cybersecurity, and authority will become increasingly shared and, hence, include both harder and softer sources. If governmental actors remain caught up in ideologically-driven disputes and fail to effectively deal with growing security concerns, 'other actors in world politics will have incentives to cooperate with each other to fill the resulting governance deficit', all the more.[945] Even as cybersecurity-related issues continue to move higher up on political agendas and crises become more acute (which would imply greater governmental control), traditional forms of state-based authority are likely to require the active assistance of non-state actors.

---

943 Kavanagh, 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (n 699) 4.

944 Ibid 4.

945 Hale (n 856) 214.

Predicting the future of the normative structures that will govern the various issues of cyberspace is difficult because of the newness and volatility of the technology, the rapid changes in economic and political interests, and the social and generational cognitive evolution that is affecting how state and non-state actors understand and define their interests. ... One projection does seem clear. It is unlikely that there will be a single overarching regime for cyberspace any time soon. A good deal of fragmentation exists now and is likely to persist.

— Joseph S. Nye Jr. *The Regime Complex for Managing Global Cyber Activities (2014)*

8 Conclusion

Contents

Against the background of steadily increasing numbers of cybersecurity incidents and ever-louder calls for measures of restraint, this thesis has aspired to uncover the roles and contributions of non-state actors to global cybersecurity norm formation processes. From architectural as well as operational standpoints, non-state actors have been at the heart of developments pertaining to networked ICTs for decades. As creators of products and suppliers of services such as end-point protection, or as owners and operators of large parts of critical network infrastructures and platforms, private protagonists have made important contributions to the security and overall design of the virtual realm.[946] Despite their de facto embeddedness in cybersecurity-related contexts, the activities of non-state actors conducted in the remit of promoting

[946] Radu (n 35); Shackelford (n 35); 30 Years of TCP and IP on Everything (n 35); Leiner and others (n 35).

responsible behaviour in cyberspace have not been studied extensively so far. This thesis has sought to offer relevant correctives.

8.1 Recapitulation and Argument

Informed by theoretical insights as well as empirical observations that normative authority has become more dispersed among different actors at the international level, and even (formerly) predominantly state-dominated realms such as security have become occupied by non-state actors, this thesis has responded to the following research question: ***How and in which capacities do non-state actors contribute to global norm construction efforts pertaining to responsible behaviour in cyberspace, and how effective is their engagement?***

Attempts to answer the research question formulated above have been grounded in assumptions that in order to increase the security of the virtual realm it is critical to understand the empirical realities and governance arrangements underlying relevant stabilising efforts.

Building on scholarship in the areas of international relations and international law and seeking to fill gaps in bodies of scholarly literatures relating to the contributions of non-state actors, this thesis has argued that the latter have come to wield considerable politico-legal influence over discussions about norms of responsible behaviour for the virtual realm. Thematic examinations of primary and secondary sources, process observations, as well as semi-structured expert interviews, have revealed seven different role profiles taken on by non-state actors in global cybersecurity norm construction projects. With reference to the case studies analysed, non-state actors have played the parts of (a) knowledge brokers, (b) awareness raisers, (c) norm leaders and cooperation incubators, (d) diplomatic change agents, (e) discussion feeders and gap fillers, (f) implementation assistants and capacity builders, as well as (g) custom shapers.

As part of the investigations conducted, this thesis has made more visible the particularities of private actor contributions to global cybersecurity governance projects. The monograph has highlighted the variegated steering parts assumed by non-state actors in cybersecurity norm formation projects, and has shown that private actors have done more than engaging in what has been termed *norm entrepreneurship*, *lobbying* or *advocacy*. In accordance with the seven role profiles identified, non-state actors have been seen to contribute to norm formation processes by means of creating information-condensing artefacts, providing subject matter expertise, or actively crafting normative proposals, among other things. In certain instances, including for example in the cases of Microsoft or the Global Commission on the Stability of Cyberspace, they have even come to behave like quasi-diplomatic actors, with access to high-ranking government channels and considerable political capital.

With a view to determining the degrees to which the activities undertaken by the non-state actors surveyed have yielded palpable results, this thesis has conducted three-tiered effectiveness evaluations. Building on legal and regime-theoretical insights, this thesis has assessed the success of their contributions across the dimensions of output, outcome, and impact. Vis-à-vis output, the non-state actors analysed have shown high degrees of effectiveness. Their policy endeavours have allowed them to markedly shape international decision-making processes pertaining to rules of the road for the digital domain, or instigate new processes which reflect their contextual and strategic preferences. In terms of outcome, politically well-connected or -endowed non-state actors have succeeded at changing intra- and inter-group behaviours, meaning the behaviours of industry fellows as well as the behaviours of other communities. Overall, however, their efforts have not (yet) scaled widely enough to have induced far-reaching systemic changes, it has been argued. While difficult to attest in causal terms, impact has been limited. However, the non-state actors examined across *Chapters 4*, *5*, and *6* have laid important foundations for further discussions about rules of

the road for cyberspace, and have provided important yardsticks for lining out the boundaries of responsible conduct in the digital domain. While they have helped bring about richer governance structures, they have also introduced new elements of complexity and fragmentation. Although the latter do not necessarily carry negative connotations per se, they have confounded accountability and legitimacy questions relating to cybersecurity norm creation ventures.

This manuscript has identified three accountability challenges arising from the roles executed by non-state actors in polycentric cybersecurity governance arrangements, namely (a) the problem of many hands, (b) the profusion of issue areas, (c) and the fluidity and malleability of institutional arrangements. These challenges, it has been argued, are the results of actor-, subject-, and venue-related elements of complexity. Indeed, rising numbers of actors, issue areas, and fora of discussion have contributed to tangled accountability structures of different texture and design, and have rendered questions, such as *which actors are responsible for which process components*, and *which entities have legitimate claims or the right to determine the norms and rules that ought to be complied with*, difficult to answer. However, with a view to inducing systemic changes in conduct, achieving far-reaching normative compliance, and enabling enforcement, untangling these accountability structures and instituting mechanisms of answerability are critical measures to pursue. Furthermore, for non-state actor-driven cybersecurity norms ventures to succeed, attaining public credibility and backing are important prerequisites.

In the absence of formal public/legal mandates to form rules of the road for the virtual realm, the non-state actors surveyed have been seen to rely on pragmatic, moral, cognitive, and knowledge-based legitimacy frames to further the acceptability of their norms-oriented undertakings. In line with the different roles executed by the non-state actors examined, as well as their respective areas of expertise, legitimacy frames used

have varied. For example, technically-oriented non-state actors, such as FIRST or Kaspersky Lab have primarily relied on scientific legitimacy frames to justify their contributions to cybersecurity norm formation processes. In contrast, economically strong and internationally well-embedded actors such as Siemens or Microsoft have used pragmatic and cognitive legitimacy frames. Social purpose corporations and academic institutions, on the other hand, have employed moral as well as knowledge-based strategies to legitimise their contributions to discussions about rules of the road for the virtual realm. This thesis has contended that authority structures are inherently fluid/liquid and that the different approaches to acquire social acceptability and credibility pursued by non-state actors imply that legitimacy is conditioned as much by 'the values, interests, expectations, and cognitive frames' of those entities who are supportive of the relevant governance endeavours as it is by the structures themselves.[947] 'As such, legitimacy can differ significantly across time and space, and between actors, systems, and contexts'.[948]

With respect to addressing the challenges identified, this manuscript has reasoned that in accordance with the distributed nature of the virtual realm, multistakeholder-oriented oversight mechanisms, as well as clear evaluation standards, and community-based responsibility anchors may provide useful starting points for encouraging more clear cut and dependable accountability structures. Given the polycentric features of debates about rules of the road for cyberspace, one-dimensional, sovereigntist accountability conceptions which intend to attach ultimate responsibility to a unitary source of authority appear ill-suited. Instead, this thesis has argued, efforts should focus on re-framing accountability structures around delineated issue areas, involving all relevant stakeholders. Higher levels of issue specificity would reduce ambiguity apropos

---

[947] Black, ''Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes' (n 43) 293.

[948] Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (n 43) 145.

actor relations, incentives, and goals, and would allow for the strategic construction and connection of different aspects and elements of cybersecurity norms debates, as well as for the attribution of stakeholder responsibilities. Furthermore, this thesis has held that clearly specified, venue-related mission statements, and openly communicated roles would go a long way with regard to establishing answerability mechanisms related to the promotion of responsible conduct in the virtual realm. While it is possible for accountability and legitimacy structures to crystallise even in environments as complex and fragmented as those pertaining to norms of responsible behaviour in cyberspace, this manuscript has acknowledged that in the near-term, they are likely to remain fluid, open to contestation, and further unsettling.

8.2 Conceptual and Empirical Contributions

From the standpoints of theory and practice, this manuscript has made several noteworthy contributions to discussions about norms of responsible behaviour in cyberspace. Joining endeavours across the disciplines of international relations and international law which have challenged state-centric conceptions of international interactions (i.e. constructivism and neo-transnationalism, respectively), this thesis has opened up and questioned dominant analytical frameworks and conceptions of agency, and has further underscored the importance of ideational factors as well as actors other than states in regulating issues of global proportions. Conceptually, thus, it has further broadened analytical grids and has offered more granular depictions of the participants present in global steering efforts. It has also presented more nuanced evaluations of the social, legal, and political processes and practices at work with regard to ensuring the security and stability of the digital domain. In addition, it has contributed to more fine-grained understandings of the different roles and charges executed by non-state actors across still fairly novel security domains (i.e. cybersecurity) by collecting and analysing primary data.

The parts played by non-traditional security agents in the digital domain, and particularly in global cybersecurity norm construction processes, have not received extensive analysis, and when addressed, have been unsuitably reduced to advocacy and lobbying endeavours. By surveying nine non-state actors concerned with cultivating norms of responsible behaviour in cyberspace across three different stakeholder clusters, this thesis has added to enhanced understandings of private inputs to complex global and security-critical steering processes. By probing more deeply into the governing roles taken on by non-governmental actors, this manuscript has also offered insights into how values are allocated globally, and has spelled out who is involved in the allocation of these values respectively. Likewise, it has theorised the implications of the roles taken on by non-state actors vis-à-vis accountability and legitimacy structures. Apart from shedding light on understudied construction processes in heterogeneous and contested normative environments, conceptually, this thesis has also demonstrated the validity of alternative regulatory approaches, including soft law and political commitments to coordinate and order global problem settings. It has drawn attention to the possibilities of soft law instruments to inspire customary practices and serve as boundary-setting instruments.

Empirically, this manuscript has presented comprehensive evidence relating to the influence exerted by non-state actors on global norm creation processes pertaining to the digital domain, as well as their strategies employed to take part in these discussions. Among other things, the results of the empirical investigations have offered practitioners opportunities to appreciate that, as non-state actors continue to be concerned about immediate and future threats to political, economic, and social systems resulting from the misuse of information and communications technologies, and consciously engage with the intention of steering activities, it is important to reconsider existing forms of interaction among different contributors as well as institutional setups.

With reference to the empirical data collected, this thesis has underscored the need for further meaningful, subject-specific forms of collaboration and cooperation

among state and non-state entities to advance debates about responsible behaviour in cyberspace and realise implementation of relevant norms. With a view to effectively responding to large-scale cybersecurity incidents, or indeed preventing such events in the first place, this thesis has maintained that it is critical for governmental structures and regulatory systems to interact with non-governmental systems in a more symbiotic fashion. Even though this thesis has criticised the dominant positions of states across international relations and international law literatures, and has highlighted the extensive parts played by non-state actors in complex governance projects, it recognises that for cybersecurity norms to have systemic effects, engagement with and support of governmental actors are baseline prerequisites. As entities with distinct public and security-related responsibilities towards their constituencies, states have critical parts to play vis-à-vis reducing risks to international peace and security in collaboration with non-state actors.

8.3 Policy Implications

Practitioners and policymakers stand to benefit from consciously taking stock of the non-state actor contributions to cybersecurity norm formation processes and reflect upon their own roles in these processes. While international deliberations concerning norms of responsible behaviour in cyberspace have proven daunting and difficult, history has shown that concurrence and progress are possible even in the most politicised and intricate of cases. Hence continued engagement on the parts of states is crucial for bringing normative efforts to fruition and maturity.

The works of the UN GGEs of 2010, 2013, and 2015 have set important precedents for normative discussions at the international level, and have served as conceptual starting points and referent objects for the non-state actor activities analysed. To increase global levels of cybersecurity and stability, and move international negotiations

forward, states have to stay committed to the spirit of the normative prescriptions developed between 2010-2015 and exercise their traditional roles as standard-setters and norm effectuators, while at the same time remaining open for new forms of collaboration and implementation in partnership with non-state actors.

In terms of stipulating voluntary norms geared towards enhancing the stability and security of the virtual realm, governmental protagonists continue to profit from a unique combination of material (access to resources and position in the global economy) and symbolic (legitimacy/ability to invoke moral claims) power sources. As such, their standard-setting capabilities continue to be of relevance. 'Failure to assign the right meaning and weight to facts, determine factors of causality in cybersecurity issues, and define appropriate remedies [would] likely ... prolong searches for shared understanding and agreement', and substantially increase the potential for escalation.[949]

To realise normative traction in the absence of concurring political standpoints, it is critical that like-minded and norms-supporting governmental protagonists deepen their enforcement capabilities to the extent that they begin to sanction irresponsible behaviour more stringently on the basis of what was agreed in the context of the UN GGE in 2015 (as has been seen in a number of public attribution statements recently). There is still no (or hardly any) sense of consequence or recrimination for violating norms of responsible behaviour in cyberspace, which casts doubts on normative guarantees uttered, and significantly increases the probability for misinterpretation and confusion. Until recently (and still), states have hidden behind a smokescreen of strategic ambiguity, and have effectively neglected their customary functions as enforcers of normative commitments. Strategic ambiguity has let governmental protagonists engage in malicious cyberactivities, including in acts of espionage, sabotage, or surveillance, without having to face punishment. However, both from tactical perspectives as

[949] Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy' (2017) ⟨https://perma.cc/Q7PD-NEJG⟩ 32.

well as from political standpoints, strategic ambiguity is risky and misleading as it does not reduce the odds for fallout.

Where substantive discussions pertaining to standards of responsible conduct in cyberspace appear inoperable, consistent state practice can offer means for further progress. Stringent state behaviour centred on observance and enforcement of proposed norms (even if only carried out by some, e.g. like-minded, states) can act as proxy for more formalised measures, and introduce much-needed red lines. For those red lines to have restraining effects, however, there needs to be credible belief of effectuation and follow-through (either directly or indirectly).

In addition to their traditional responsibilities, governmental protagonists have to assume new roles. In light of increasing non-state actor engagement in processes of global cybersecurity norm development, there is scope for reconfigurations of sovereign functions. While the 2013 and 2015 UN GGE reports did not specify rules of engagement between state and non-state actors, they did acknowledge that there is merit in establishing, and where applicable, expanding linkages among these entities. It was noted, for example, that while sovereign protagonists bear primary responsibilities for national security and the safety of their citizens, including in the digital realm, international cooperation and cross-sectoral assistance are critical with regard to enabling states to secure ICTs and warrant their peaceful use. 'Assistance to build capacity in ICT security is also essential for international security, by improving states' capacity for cooperation and collective action'.[950] Given that as much as 80% of critical network infrastructures are owned and/or operated by private sector companies, and that non-state actors are actively injecting their views and proposals into international cybersecurity norm development processes, states have to start engaging as sparring partners of non-state initiatives and delegators of normative responsibilities. The latter

[950] James Andrew Lewis, UN Publishes Latest Report of the Group of Government Experts (2015) ⟨https://perma.cc/V5WD-DPDN⟩ accessed 21 August 2018.

suggests a pooling or sharing of traditional responsibilities with private actors vis-a-vis the development and application (putting into practice) of international standards for responsible behaviour in cyberspace, while the former involves an extension of public support for non-state actor-driven efforts.

For the norms-based efforts underway since the late 1990s and the non-state activities surveyed as part of this thesis to achieve systemic effects and increase the security and stability of the virtual realm, governmental and non-governmental actors are well advised to apply alliance-oriented postures. Rather than focusing on the emergence of stable and unanimous blocs seeking alignment across the full spectrum of cybersecurity norms-related issues, progress is likely to be more palpable on the bases of different constellations of actors which assemble around shared issue-specific areas, e.g., vulnerabilities disclosure processes, or critical infrastructure protection in the healthcare sector. In terms of policy, this means that progress is likely to be multi-staged and that case-specific thinking is needed with regard to identifying the relevant actors with 'the willingness and capacity to lead on' specific issue areas.[951]

As has been discussed as part of the previous chapter, issue-centric approaches also entail (re-)evaluations of legitimacy and accountability structures. Hence with a view to attaining and evaluating security in the virtual realm, 'there is a need to focus on not just interests and leadership, but also followership'.[952] And as the case studies have evidenced, in the context of promoting norms of responsible behaviour in cyberspace 'potential leaders include private or non-state actors and fully private or public–private multistakeholder bodies while potential followers often include states and multilateral organisations'.[953]

---

[951] Breslin and Nesadurai (n 44) 199.

[952] Ibid 199.

[953] Ibid 199.

8.4 Avenues for Further Research and Outlook

In line with the overarching goal of this thesis to better understand the contributions of non-state actors to traditionally state-driven governance processes, readers have been presented with comprehensive insights into the different role profiles executed by private actors in cybersecurity norm development processes. While this thesis has aspired to answer the stated research question as expansively as possible, there remain numerous opportunities for further research. The following paragraphs highlight four specific opportunities for further academic contributions.

With regard to the empirical aspects of this thesis, for instance, future analytical endeavours could extend the scope of cases selected for examination, and add to the findings of this thesis, both in terms of relevant actors partaking in cybersecurity norm formation ventures as well as in terms of roles executed. Investigating whether and how less vocal non-state actors participate in debates about rules of the road for cyberspace may reveal additional types of governance roles taken on by private actors. Endeavours geared towards studying additional cases could centre on applying stronger stakeholder cluster or regional focal points, and could for instance survey which and how civil society organisations in the Global South contribute to rules of the road for the virtual realm. Efforts of this nature could help deepen insights into non-traditional modes of governance in the area of cybersecurity and the processes through which non-state actors seek to engage and achieve policy results across different regional contexts, and may make up for participatory shortcomings on the parts of governmental actors.

Furthermore, future research endeavours could also conduct policy-near research pertaining to frameworks for measuring effectiveness, and work on developing relevant key performance indicators and metrics. Reliable data on non-state actor-driven norm formation ventures (as well as state-driven undertakings) and effects realised by these ventures have been scarce. With a view to operationalising normative stipulations issued

by private actors as well as achieving greater levels of security and stability in cyberspace, being able to determine courses of action based on dependable, data-driven sources of information is critical. Future academic undertakings could help establish relevant sources of data in the form of repositories, and actively shape the development of norms-related metrics, both qualitative and quantitative in nature. The interviews conducted as part of this thesis have confirmed the glaring absence of norms-related evaluation frameworks and the lack of relevant indicators to contextualise the activities undertaken by non-state actors vis-à-vis promoting rules of the road for the virtual realm.

In addition, future scholarly examinations could study power-related dynamics resulting from private cybersecurity norm-making efforts. This thesis has shown that in the context of promoting rules of the road for the virtual realm, non-state actors have come to influence decision-making processes, discourses, and rule-making endeavours, i.e. they have come to exert considerable decisional, discursive, and regulatory power.[954] As the case studies have evidenced, non-state actors have carved out contributory spaces and have purposefully and authoritatively employed their specific competencies to add to and steer global debates pertaining to norms of responsible behaviour in cyberspace. Against the background of these realities, scholars interested in global power constellations, e.g. political scientists, could further dissect the implications of non-state actor contributions on central aspects of (political) authority. The results of this thesis would go to suggest the presence of less formal/traditional sources of political authority, as well as altered power configurations which could potentially imply the need for different forms of interaction and cooperation.

More theoretically oriented ventures could attempt to unveil the mechanisms and key factors required for supporting norms adoption and operationalisation processes in the context of promoting responsible behaviour in cyberspace. Scholarly research on

[954] Arts (n 231).

incentivisation mechanisms and frameworks has remained underdeveloped. However, in light of proliferating cybersecurity incidents targeting critical infrastructures, including hospitals and medical research facilities, for example, and in the interest of increasing the stability of the virtual realm, more research around incentivisation modalities is urgently needed. There is theoretical and practical value in identifying the underlying logics and processes for stipulating norms adherence, as well as in evaluating means for addressing and sanctioning non-conformity. To curb malicious activities in the virtual realm it is necessary to change existing calculi pertaining to normative non-adherence/selective adherence. What Ruhl and others have maintained with reference to governmental actors namely that '[f]or states to internalise norms, they must perceive the prospective benefits of adherence (in terms of concrete benefits for adopting or the costs that may follow failure to do so) as outweighing the prospective benefits of remaining outside of normative constraints' also holds true for non-state actors.[955] Identifying mechanisms and levers with the potential to shift existing calculi favouring non-adherence and foster more consequential postures on the parts of governmental as well as non-governmental actors vis-à-vis calling out violations would help norms attain more systemic effects.

Although the norms-related activities pursued by non-state actors have struggled to induce large-scale, systemic effects with regard to increasing the security of cyberspace (so far), they have been important in and of themselves. Among other things, the efforts conducted by non-state actors have contextualised and diversified discussions, have increased the substantial scope of debates, and have built momentum for further engagements. This thesis has intended to aid the progression of debates about rules of the road for cyberspace by offering more refined understandings of and appreciation for the roles of non-state actors, both from theoretical as well as practical viewpoints. As governmental endeavours continue to be challenged and destabilised

[955] Ruhl and others (n 314) 16.

by conflicting, ideologically-framed national interests, persistent engagement on the parts of non-state actors will be critical for debates about rules of the road to advance further. As aptly noted by Hollis and Neutze in their research paper on *Defending Democracies via Cybernorms*,

> [c]areful cultivation and strategic choices will be required to move from normative ideas to fully internalised sets of behavioural expectations for relevant actors. And it may be the case, that other cybernorm projects and those focused on their implementation and adherence will be needed in the future to address shifting tools and techniques.[956]

As the findings of this thesis have shown, by taking on various critical steering roles beyond advocacy and lobbying, private actors will serve as important accelerators and multipliers for implementing norms of responsible behaviour in cyberspace, and may even take on implementation-related activities themselves, e.g. by means of operationalising norms technically, that is, by developing and implementing technical standards/computer code which reflect normative contents. 'Simply put, technical solutions may exist to advance the adoption or diffusion of certain cybernorms'.[957] Although not endowed with formal law-making capabilities under positivist notions of international law and international relations, the work of non-state actors has proven to be and will continue to be exceptionally important in terms of lining out and shaping the boundaries of responsible conduct in cyberspace and ensuring adequate levels of security and stability.

---

[956] Duncan B Hollis and Jan Neutze, 'Defending Democracies via Cybernorms' (Philadelphia, PA, 2020) ⟨https://perma.cc/457E-XQKH⟩ 40.

[957] Ruhl and others (n 314) 19.

Cyberspace is getting larger, not smaller. Its influence on international relations is growing not shrinking. So, it is ever more important ... to do what we can to ensure the law applies in cyberspace too.

— Jeremy Wright, *Cyber and International Law in the 21st Century (2018)*

9 Appendices

Contents

9.1 Appendix Chapter 1

The list below provides an overview of the author's works published over the course of writing this thesis. Some of the works published have been integrated in full or in part as sections into this monograph.

- Jacqueline Eggenschwiler, Ioannis Agrafiotis, and Jason RC Nurse, 'Insider Threat Response and Recovery Strategies in Financial Services Firms' (2016) 2016(11) Computer Fraud & Security 12 ⟨https://perma.cc/L29A-H56C⟩.
- Jacqueline Eggenschwiler, 'Accountability Challenges Confronting Cyberspace Governance' (2017) 6(3) Internet Policy Review 1 ⟨https://perma.cc/3KT6-SHGP⟩.

- Jacqueline Eggenschwiler, 'A Typology of Cybersecurity Governance Models' (2018) 13(2) St Antony's International Review 64 ⟨https://perma.cc/4AK4-JGUU⟩.
- Jacqueline Eggenschwiler, *Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector Framework Document* (techspace rep, Geneva Dialogue on Responsible Behaviour in Cyberspace 2018) ⟨https://perma.cc/3WKN-BFH4⟩.
- Jacqueline Eggenschwiler and Jantje Silomon, 'Challenges and Opportunities in Cyber Weapon Norm Construction' (2018) 2018(12) Computer Fraud & Security 11 ⟨https://perma.cc/CK9P-CK47⟩.
- Jacqueline Eggenschwiler, 'An Incident-Based Conceptualization of Cybersecurity Governance' in Ryan Ellis and Vivek K Mohan (eds), *Rewired: Cybersecurity Governance* (John Wiley & Sons 2019).
- Myriam Dunn Cavelty and Jacqueline Eggenschwiler, Behavioral Norms in Cyberspace: Can Corporations Make the Digital Sphere Secure? (2019) ⟨https://perma.cc/4GQE-EWVR⟩ accessed 10 December 2019.
- Jacqueline Eggenschwiler, *International Cybersecurity Norm Development: The Roles of States Post-2017* (techspace rep, April, EU Cyber Direct 2019) ⟨https://perma.cc/7PR4-C72T⟩.
- Jacqueline Eggenschwiler, 'Expert Commissions and Norms of Responsible Behaviour in Cyberspace: A Review of the Activities of the GCSC' [2020] Digital Policy, Regulation and Governance ⟨https://perma.cc/4QKH-F2WG⟩.
- Jacqueline Eggenschwiler and Joanna Kulesza, 'Non-State Actors as Shapers of Customary Standards of Responsible Behaviour in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020).

9.2 Appendix Chapter 3

9.2.1 Interview Guide

The list below provides an overview of the questions included in the interview guide.

- Why do non-state actors, such as ... engage in norm-making processes?
- How do non-state actors (or specific actor ...) engage?
- How does ... see its role(s)? What does ... consider its role(s) to be?
- What are the benefits and drawbacks of non-state actor engagement?

- What does non-state actor engagement mean for the broader cybersecurity governance debate?
- How did consensus about the ... (relevant norms proposal) come about?
- How can the norms proposed, be adopted and meaningfully enforced? What do you consider to be the main challenges for effective implementation/enforcement?
- How are other stakeholders involved and how do they contribute?
- How successful is ... in terms of promoting the peaceful use of cyberspace, and what are the measures of effectiveness applied?
- Is impact pertaining to the activities undertaken measured somehow, and if so, how?
- How are legitimacy considerations taken into account? What does ... consider itself to be accountable for?
- Whom does ... consider to be its key accountability stakeholders? Whom does it owe account to and how is accountability being rendered?
- Are there areas of policy or debate more generally, where you would deem involvement of ... off the table?
- How do you expect the norms debate to advance?

9.2.2 List of Interviewees

The table below provides an overview of the interviews conducted as part of this thesis.

Table 9.1: List of Interviewees.

Interviewee	Gender	Stakeholder Group	Interview Location	Date
Expert #1	Male	Expert Community	VoIP	2019-06-03
Expert #2	Female	Civil Society	EuroDIG	2019-06-19
Expert #3	Male	Industry	EuroDIG	2019-06-19
Expert #4	Female	Industry	EuroDIG	2019-06-19
Expert #5	Male	Civil Society	EuroDIG	2019-06-20
Expert #6	Female	Academia	EuroDIG	2019-06-20
Expert #7	Male	Industry	VoIP	2019-06-27
Expert #8	Male	Industry	VoIP	2019-06-28
Expert #9	Female	Expert Community	VoIP	2019-06-28
Expert #10	Male	Government	VoIP	2019-07-01
Expert #11	Male	Expert Community	VoIP	2019-07-02

Continued on next page

Table 9.1 – continued from previous page

Interviewee	Gender	Stakeholder Group	Interview Location	Date
Expert #12	Male	Industry	VoIP	2019-07-02
Expert #13	Female	Civil Society	VoIP	2019-07-06
Expert #14	Female	Civil Society	VoIP	2019-07-08
Expert #15	Male	Academia	VoIP	2019-07-12
Expert #16	Male	Expert Community	VoIP	2019-07-16
Expert #17	Female	Academia	VoIP	2019-07-19
Expert #18	Male	Industry	VoIP	2019-07-19
Expert #19	Male	Civil Society	VoIP	2019-07-22
Expert #20	Male	Expert Community	VoIP	2019-07-26
Expert #21	Male	Industry	VoIP	2019-07-29
Expert #22	Male	Industry	VoIP	2019-07-31
Expert #23	Male	Expert Community	VoIP	2019-08-08
Expert #24	Male	Civil Society	VoIP	2019-08-26
Expert #25	Male	Industry	VoIP	2019-08-27
Expert #26	Female	Academia	VoIP	2019-10-11
Expert #27	Male	Expert Community	VoIP	2019-10-11
Expert #28	Male	Expert Community	VoIP	2019-10-28
Expert #29	Female	Academia	VoIP	2019-10-31
Expert #30	Male	Civil Society	VoIP	2019-11-07
Expert #31	Female	Academia	VoIP	2019-11-20
Expert #32	Male	Expert Community	VoIP	2020-01-10

9.3 Appendix Chapter 4

The table below provides an overview of the members of the second International Group of Experts.

Table 9.2: Members of the Second International Group of Experts.

Expert	Designation	Affiliation
Prof. Dapo Akande	Professor of Public International Law	University of Oxford, UK
Col. Gary D. Brown	Professor for Cybersecurity	Marine Corps University, US
Prof. (Brigadier General) Paul Ducheine	Professor for Military Law of Cybersecurity and Cyberoperations	University of Amsterdam, The Netherlands
Prof. Terry D. Gill	Professor for Military Law	University of Amsterdam, The Netherlands
Prof. Wolff Heintschel von Heinegg	Professor of Public International Law	Europa-Universität Viadrina, Germany

Continued on next page

Table 9.2 – continued from previous page

Expert	Designation	Affiliation
Dr. Gleider I. Hernández	Associate Professor of Public International Law	Durham University School of Law, UK
Deborah Housen-Couriel	Research Fellow	University of Haifa Faculty of Law, Israel
Prof. Zhixiong Huang	Deputy Director of the Institute of International Law	Wuhan University Institute of International Law, China
Prof. Eric Talbot Jensen	Professor of Law	Brigham Young University Law School, US
Prof. Kriangsak Kittichaisaree	Member of the International Law Commission of the United Nations	United Nations
Andrey L. Kozik	Associate Professor for International Law	KIMEP University, Kazakhstan
Prof. Claus Kreß	Professor of International Law and Criminal Law	University of Cologne, Germany
Prof. Tim McCormack	Professor of Law and Dean of the Faculty of Law	University of Tasmania, Australia
Prof. Kazuhiro Nakatani	Professor of International Law	University of Tokyo, Japan
Gabor Rona	Professor of Practice	Cardozo School of Law (formerly International Legal Director of Human Rights First), US
Phillip Spector	Formerly Senior Adviser to the Legal Adviser	Department of State, US
Prof. Sean Watts	Professor of Law	Creighton University School of Law, US
Dr. Bernhards Blumbergs	Technology Researcher	NATO Cooperative Cyber Defence Centre of Excellence, Estonia
Steven Hill	Legal Adviser and Director of the Office of Legal Affairs	NATO, Belgium

9.4 Appendix Chapter 5

The table below provides an overview of the members of the Charter of Trust.

Table 9.3: Members of the Charter of Trust.

Signatory	Sector Affiliation	Further Sponsorship
Siemens	Industrial Manufacturing	Paris Call for Trust and Security in Cyberspace
Munich Security Conference	Conference	N/A
AES	Energy	Paris Call for Trust and Security in Cyberspace
Airbus	Aviation	Paris Call for Trust and Security in Cyberspace
Allianz	Insurance	Paris Call for Trust and Security in Cyberspace
Atos	IT Services	Paris Call for Trust and Security in Cyberspace
Cisco	Networking (IT)	Paris Call for Trust and Security in Cyberspace, Cybersecurity Tech Accord
Daimler (left the Charter of Trust in February 2020)	Automotive	Paris Call for Trust and Security in Cyberspace
Dell Technologies	Hardware	Paris Call for Trust and Security in Cyberspace, Cybersecurity Tech Accord
Deutsche Telekom	Telecommunication	Paris Call for Trust and Security in Cyberspace
Enel (left the Charter of Trust in February 2019)	Energy	Paris Call for Trust and Security in Cyberspace
IBM	IT Services	Paris Call for Trust and Security in Cyberspace
Infineon Technologies AG	Semiconductors	Paris Call for Trust and Security in Cyberspace
Mitsubishi Heavy Industries	Engineering	N/A
NXP	Semiconductors	Paris Call for Trust and Security in Cyberspace
NTT	IT Services	N/A
SGS	Certification	Paris Call for Trust and Security in Cyberspace
Total	Energy	Paris Call for Trust and Security in Cyberspace
TÜV Süd	Certification	Paris Call for Trust and Security in Cyberspace
German Federal Office for Information Security (BSI)	Federal Agency	N/A
CCN National Cryptologic Centre of Spain	Intelligence	N/A
Graz University of Technology	Academia	N/A

Continued on next page

Table 9.3 – continued from previous page

Signatory	Sector Affiliation	Further Sponsorship
Hasso Plattner Institute for Digital Engineering GmbH (HPI)	IT Institute	N/A

9.5 Appendix Chapter 6

The table below provides an overview of the members of the Global Commission on the Stability of Cyberspace.

Table 9.4: Members of the Global Commission on the Stability of Cyberspace.

Commissioner	Country	Position	GCIG
Michael Chertoff	US	Chair, Former Secretary of Homeland Security	Yes
Latha Reddy	India	Chair, Former Deputy National Security Adviser of India	Yes
Marina Kaljurand	Estonia	Former Chair (February 2017-March 2019), Former Foreign Minister and Ambassador of Estonia	No
Abdul-Hakeem Ajijola	Nigeria	Chair of the Working Group on Cyber Incident Management and Critical Information Protection of the Global Forum on Cyber Expertise	No
Virgilio Almeida	Brazil	Former National Secretary for Information Technology Policies of Brazil	Yes
Isaac Ben-Israel	Israel	Head of the Blavatnik Interdisciplinary Cyber Research Center of Tel-Aviv University	No
Scott Charney	US	Vice President for Security Policy at Microsoft	No
Frédérick Douzet	France	Professor at the French Institute of Geopolitics at Paris 8 University	No
Anriette Esterhuysen	South Africa	Executive Director of the Association for Progressive Communications	Yes
Jane Holl Lute	US	Special Coordinator on Improving the United Nations Response to Sexual Exploitation and Abuse	No

Continued on next page

Table 9.4 – continued from previous page

Commissioner	Country	Position	GCIG
Nigel Inkster	UK	Senior Advisor at the International Institute for Strategic Studies	No
Khoo Boon Hui	Singapore	Former Senior Deputy Secretary of the Ministry of Home Affairs of Singapore	No
Wolfgang Kleinwächter	Germany	Former Board Member of ICANN and Special Ambassador of the NETMundial Initiative	No
Olaf Kolkman	The Netherlands	Chief Internet Technology Officer at Internet Society	Yes
Lee Xiaodong	China	Founder and President of the Fuxi Institution on Internet Innovation and Development	No
James Lewis	US	Senior Vice President and Program Director at the Center for Strategic and International Studies	No
Jeff Moss	US	Chief Executive Officer of DEF CON and Chief Security Officer/Vice President of ICANN	No
Elina Noor	Malaysia	Visiting Fellow at the Institute of Strategic and International Studies Malaysia	No
Joseph S. Nye, Jr.	US	University Distinguished Service Professor, Emeritus and former Dean of the Harvard's Kennedy School of Government	Yes
Christopher Painter	US	Former Coordinator for Cyber Issues for the US Department of State	No
Uri Rosenthal	The Netherlands	Former Minister of Foreign Affairs of the Netherlands	Yes
Ilya Sachkov	Russia	Chief Executive Officer at Group-IB	No
Samir Saran	India	President of the Observer Research Foundation	No
Marietje Schaake	The Netherlands	Member of the European Parliament for the Dutch Democratic Party (D66)	Yes
Motohiro Tsuchiya	Japan	Deputy Director at Keio University Global Research Institute	No
Bill Woodcock	US	Executive Director at Packet Clearing House	Yes

Continued on next page

Table 9.4 – continued from previous page

Commissioner	**Country**	**Position**	**GCIG**
Zhang Li	China	Assistant President of China Institutes of Contemporary International Relations	No
Jonathan Zittrain	US	George Bemis Professor of International Law at Harvard Law School and the Harvard Kennedy School of Government	No

What is certain is that the development of cybersecurity norms will be a long process. Progress in some areas need not wait for progress in others.

— Joseph S. Nye, *How Will New Cybersecurity Norms Develop? (2018)*

Bibliography

Abbott KW and Snidal D, 'Hard and Soft Law in International Governance' (2000) 54(3) International Organization 421 ⟨https://perma.cc/584R-7QB7⟩.

— 'The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State', in W Mattli and N Woods (eds), *The Politics of Global Regulation* (Princeton University Press 2009) ⟨https://perma.cc/7DCF-KZFV⟩.

Accenture and Ponemon Institute, *Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection* (techspace rep, 2019) ⟨https://perma.cc/LQ77-MW9H⟩.

Adams WC, Conducting Semi-Structured Interviews (Wiley Online Books, 2015) ⟨https://perma.cc/S78L-LVUP⟩.

Aiken K, Ready to Respond to the Cyber Norms Debate (2018) ⟨https://perma.cc/WP2E-C9RL⟩ accessed 28 August 2020.

Aitken R, Global Information Security Spending to Exceed $124B in 2019, Privacy Concerns Driving Demand (2018) ⟨http://perma.cc/Q9ER-K8SJ⟩ accessed 3 April 2019.

Albin C, 'Can NGOs Enhance the Effectiveness of International Negotiation?' (1999) 4(3) International Negotiation 371 ⟨https://perma.cc/A59H-CUAV⟩.

Allen M, *The SAGE Encyclopedia of Communication Research Methods* (SAGE Publications, Inc 2017).

Alston P, *Non-State Actors and Human Rights* (Collected Courses of the Academy of European Law, Oxford University Press 2005).

Anderson C, 'Presenting and Evaluating Qualitative Research' (2010) 74(8) American Journal of Pharmaceutical Education 141 ⟨https://perma.cc/ADF7-HM28⟩.

Andonova LB, Betsill MM, and Bulkeley H, 'Transnational Climate Governance' (2009) 9(2) Global Environmental Politics 52 ⟨https://perma.cc/B8B4-WJKZ⟩.

Applegate S, 'Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare' (2011) 9(5) IEEE Security & Privacy Magazine 16 ⟨https://perma.cc/2LF4-V229⟩.

Arimatsu L, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' [2012] (September 2011) 4th International Conference on Cyber Conflict 91 ⟨https://perma.cc/PNN2-JXL4⟩.

Arquilla J and Ronfeldt D, 'Cyberwar Is Coming!' (1993) 12(2) Comparative Strategy 141 ⟨https://perma.cc/4JEZ-W5U8⟩.

Arts B, 'Non-State Actors in Global Governance: Three Faces of Power' (2003) ⟨https://perma.cc/9TF3-F9VU⟩.

Arts B, Noortmann M, and Reinalda B, *Non-State Actors in International Relations* (Ashgate 2001).

Association for Progressive Communications, Civil Society Statement to the UN General Assembly First Committee on Disarmament and International Security on Cyber Peace and Human Security (2019) ⟨https://perma.cc/2A8F-CDSC⟩ accessed 29 August 2020.

— APC Statement at the UN Open-ended Working Group on International Cybersecurity (2020) ⟨https://perma.cc/46MY-8X8E⟩ accessed 29 August 2020.

Attride-Stirling J, 'Thematic Networks: An Analytic Tool for Qualitative Research' (2001) 1(3) Qualitative Research 385 ⟨https://perma.cc/CG4E-GKYS⟩.

Baldwin DA, *The Concept of Security* (vol 23, 1997) ⟨https://perma.cc/6GNA-9N69⟩.

Balzacq T and Dunn Cavelty M, 'A Theory of Actor-Network for Cyber-Security' (2016) 1(2) European Journal of International Security 176 ⟨https://perma.cc/5JTM-RMYC⟩.

Bandola-Gill J and Lyall C, 'Knowledge Brokers and Policy Advice in Policy Formulation' in M Howlett and I Mukherjee (eds), *Handbook of Policy Formulation* (Edward Elgar Publishing Ltd 2017).

Barlow JP, A Declaration of the Independence of Cyberspace (1996) ⟨https://perma.cc/DRJ9-WEGT⟩ accessed 19 November 2019.

Barnsby RE and Reeves SR, 'Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter' (2017) 95(7) Texas Law Review ⟨https://perma.cc/H3KQ-Z728⟩.

Bauer M and Gaskell G, *Qualitative Researching with Text, Image and Sound* (Bauer MW and Gaskell GD eds, SAGE Publications Ltd 2000).

BBC News, German Politicians Targeted in Mass Data Attack (2019) ⟨https://perma.cc/K7MQ-SAC9⟩ accessed 11 April 2019.

BDO, *Top Ten Trends and Key Reccommendations for 2019* (techspace rep, 2018) ⟨https://perma.cc/RUK7-YBBM⟩.

— *Cyber Security in 2020: Top Ten Predictions and Recommendations* (techspace rep, 2019) ⟨https://perma.cc/5TD3-LHVL⟩.

Behravesh M, Constructivism: An Introduction (2011) ⟨https://perma.cc/V9RL-CGL4⟩ accessed 9 February 2018.

Beisheim M and Liese A, 'Research Design: Measuring and Explaining the Effectiveness of PPPs' in *Transnational Partnerships* (Palgrave Macmillan UK 2014).

Belli L and Venturini J, 'Private Ordering and the Rise of Terms of Service as Cyber-Regulation' (2016) 5(4) Internet Policy Review 1 ⟨https://perma.cc/YM44-VW2G⟩.

Bequerel S, Kaspersky au Paris Peace Forum (2019) ⟨https://perma.cc/5TV5-LG2Z⟩ accessed 28 August 2020.

Betsill MM and Corell E, 'NGO Influence in International Environmental Negotiations: A Framework for Analysis' (2001) 1(4) Global Environmental Politics 65 ⟨https://perma.cc/W2E6-97VX⟩.

Bhattacherjee A, Interpretive Research (2019) ⟨http://perma.cc/3GSN-TKAL⟩ accessed 17 March 2019.

Bianchi A, 'The Fight for Inclusion: Non-State Actors and International Law' in *From Bilateralism to Community Interest* (Oxford University Press 2011) ⟨https://perma.cc/R285-SK6V⟩.

Black J, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54(1) Current Legal Problems 103 ⟨https://perma.cc/6XKU-KDYK⟩.

— 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (February, London, 2008) ⟨https://perma.cc/6W4J-NKKV⟩.

— ''Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes' (2017) 9(2) International Theory 286 ⟨https://perma.cc/3Y2Z-GEBC⟩.

Black J, Hopper M, and Band C, 'Making a Success of Principles-Based Regulation' (2007) 1(3) Law and Financial Markets Review 191 ⟨https://perma.cc/NRR2-MZCU⟩.

Boswell C, 'The Political Functions of Expert Knowledge: Knowledge and Legitimation in European Union Immigration Policy' (2008) 15(4) Journal of European Public Policy 471 ⟨https://perma.cc/338R-JB48⟩.

Bovens M, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13(4) European Law Journal 447 ⟨https://perma.cc/775V-AJQU⟩.

Bovens M, Goodin RE, and Schillemans T, 'Public Accountability' in M Bovens, RE Goodin, and T Schillemans (eds), *The Oxford Handbook of Public Accountability* (Oxford University Press 2014) ⟨https://perma.cc/CMF8-UUBZ⟩.

Bowen GA, 'Document Analysis as a Qualitative Research Method' (2009) 9(2) Qualitative Research Journal 27 ⟨https://perma.cc/5MT5-W8MY⟩.

Braun V and Clarke V, 'Using Thematic Analysis in Psychology' (2006) 3(2) Qualitative Research in Psychology 77 ⟨https://perma.cc/9H67-93JB⟩.

Brenner J, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press 2011).

— *Keeping America Safe. Toward More Secure Networks for Critical Sectors* (techspace rep, Massachusetts Institute of Technology 2017) ⟨https://perma.cc/UJ27-JE4Y⟩.

Breslin S and Nesadurai HES, 'Who Governs and How? Non-State Actors and Transnational Governance in Southeast Asia' (2018) 48(2) Journal of Contemporary Asia 187 ⟨https://perma.cc/XP74-3MLF⟩.

Bresnahan T, 'General Purpose Technologies' in BH Hall and N Rosenberg (eds), *Handbook of the Economics of Innovation* (Elsevier Science 2010).

Bricker D, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust* (techspace rep, Ipsos 2018) ⟨https://perma.cc/Z4TA-LACZ⟩.

Broeders D, *The Public Core of the Internet: An International Agenda for Internet Governance* (The Netherlands Scientific Council for Government Policy ed, Amsterdam University Press 2016) ⟨https://perma.cc/S4NN-LEDQ⟩.

— 'Aligning the International Protection of the Public Core of the Internet with State Sovereignty and National Security' (2017) 2(3) Journal of Cyber Policy 366 ⟨https://perma.cc/8X93-CMUR⟩.

— *Defining the Protection of the Public Core of the Internet as a National Interest* (techspace rep, 190, ORF Issue Brief 2017).

Brooks S and others, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (techspace rep, National Institute of Standards and Technology 2017) ⟨https://perma.cc/DH89-EAAL⟩.

Brunnée J and Toope SJ, 'Constructivism and International Law' in JL Dunoff and MA Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations* (Cambridge University Press 2013) ⟨https://perma.cc/ZN62-NCZA⟩.

Bryman A, *Social Research Methods* (5th edn, Oxford University Press 2015).

Buchan R, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) Journal of Conflict and Security Law 429 ⟨https://perma.cc/N358-6C9L⟩.

Burns B, Carnegie Endowment for International Peace (2020) ⟨https://perma.cc/42K7-FB6S⟩ accessed 28 August 2020.

Burris SC, Drahos P, and Shearing CD, 'Nodal Governance' (2005) 30 Australian Journal of Legal Philosophy 1 ⟨https://perma.cc/2GTR-H69Q⟩.

Burt T, CyberPeace Institute Fills a Critical Need for Cyberattack Victims (2019) ⟨https://perma.cc/3Y6C-RTQX⟩ accessed 6 March 2020.

Busé MS, 'Non-State Actors and Their Significance' (2001) 5(3) Journal of Mine Action ⟨https://perma.cc/CXL3-LYRS⟩.

Busemann H.-E and Hummel T, German Politicians' Data Published Online in Massive Breach (2019) ⟨https://perma.cc/E72S-NJQZ⟩ accessed 2 April 2019.

Buzan B, Wæver O, and Wilde J de, *Security: A New Framework for Analysis* (Lynne Rienner 1998).

Cabinet Office, *Cyber Security Strategy of the United Kingdom* (techspace rep, June, 2009) ⟨https://perma.cc/SE9M-QTPW⟩.

Calhoun C, *Dictionary of the Social Sciences* (Calhoun C ed, October, Oxford University Press 2002) ⟨https://perma.cc/2R32-TBBY⟩.

Campbell JL and Pederson OK, *The National Origins of Policy Ideas: Knowledge Regimes in the United States, France, Germany, and Denmark* (Princeton University Press 2014).

Capgemini, Capgemini Joins Cybersecurity Tech Accord (2018) ⟨https://perma.cc/DT4V-LAEW⟩ accessed 28 August 2020.

Carnegie Endowment for International Peace, Cyber Norms Index (2017) ⟨https://perma.cc/EV2T-4BXQ⟩ accessed 9 November 2017.

Carnegie Endowment for International Peace, Cyber Norms Revisited: International Cybersecurity and the Way Forward (2017) ⟨https://perma.cc/W89H-ZL53⟩ accessed 9 November 2017.

— '2019 Annual Report' [2020] 2019 Annual Report ⟨https://perma.cc/Q6XF-D3ZZ⟩.

— About Carnegie (2020) ⟨https://perma.cc/3392-WSNC⟩ accessed 28 August 2020.

— About the FinCyber Strategy Project (2020) ⟨https://perma.cc/ZJ2K-RLAY⟩ accessed 28 August 2020.

— Cyber Policy Initiative (2020) ⟨https://perma.cc/B5LT-JBHJ⟩ accessed 28 August 2020.

— Cyber Resilience and Financial Organisations: A Capacity-Building Tool Box (2020) ⟨https://perma.cc/CY9H-G9MR⟩ accessed 28 August 2020.

— G20 Proposal (2020) ⟨https://perma.cc/DEC3-T93R⟩ accessed 28 August 2020.

— International Cybersecurity Norms (2020) ⟨https://perma.cc/P7TP-YKU3⟩ accessed 28 August 2020.

Carr M, 'Public-Private Partnerships in National Cybersecurity Strategies' (2016) 92(1) International Affairs 43 ⟨https://perma.cc/KJ8J-EW6J⟩.

Carraro V, 'Electing the Experts: Expertise and Independence in the UN Human Rights Treaty Bodies' (2019) 25(3) European Journal of International Relations 826 ⟨https://perma.cc/8DS3-68YV⟩.

Carson CD and others, 'Philosophy of Research' in *Qualitative Marketing Research* (SAGE Publications, Ltd 2001).

cc P, About (2020) ⟨https://perma.cc/9WJT-2T7T⟩ accessed 29 January 2020.

Center for Strategic and International Studies, *Significant Cyber Incidents Since 2006* (techspace rep, 2019) ⟨https://perma.cc/PP76-EQA5⟩.

Charter of Trust, Charter of Trust: For a Secure Digital World (2018) ⟨https://perma.cc/ZNQ6-UCZ5⟩ accessed 11 July 2018.

— Driving Security in An Insecure World (2020) ⟨https://perma.cc/2EC3-73HX⟩ accessed 28 August 2020.

— *Seeing Cybersecurity as an Opportunity* (techspace rep, Charter of Trust 2020) ⟨https://perma.cc/H56C-DFTS⟩.

Chatham House, Global Commission on Internet Governance (2019) ⟨https://perma.cc/F99V-44CN⟩ accessed 25 November 2019.

Checkel JT, 'Norms, Institutions, and National Identity in Contemporary Europe' (1999) 43(1) International Studies Quarterly 83 ⟨https://perma.cc/ZA9H-BA76⟩.

— 'Constructivism and Foreign Policy', in S Smith, A Hadfield, and T Dunne (eds), *Foreign Policy: Theories, Actors, Cases* (Oxford University Press 2008).

Choucri N and Clark DD, 'Integrating Cyberspace and International Relations: The Co-Evolution Dilemma' [2012] (29) SSRN Electronic Journal 1 ⟨https://perma.cc/9LZ8-SLGA⟩.

Citizen Lab, NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases (2019) ⟨https://perma.cc/H9JG-98C5⟩ accessed 3 September 2020.

— About the Citizen Lab (2020) ⟨https://perma.cc/F2VE-VH7H⟩ accessed 29 August 2020.

Clapham A, 'Non-State Actors' in *International Human Rights Law* (April, Oxford University Press 2013) ⟨https://perma.cc/B8JZ-6VND⟩.

Clarke RA and Knake R, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins 2010).

Coleman EG, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso 2014).

Conklin J and others, 'Knowledge Brokers in a Knowledge Network: The Case of Seniors Health Research Transfer Network Knowledge Brokers' (2013) 8(1) Implementation Science 7 ⟨https://perma.cc/L3FH-CJNJ⟩.

Corell E and Betsill MM, 'Analytical Framework: Assessing the Influence of NGO Diplomats' in *NGO Diplomacy* (2007, The MIT Press 2007) ⟨https://perma.cc/6EV3-4YP6⟩.

Corn G, Tallinn Manual 2.0 – Advancing the Conversation (2017) ⟨https://perma.cc/2ZR9-54FX⟩ accessed 29 August 2020.

Cornish P and Kavanagh C, *Geneva Dialogue on Responsible Behaviour Phase One Report* (techspace rep, 2019) ⟨https://perma.cc/7P95-Z2DZ⟩.

Cornut J, 'The Practice Turn in International Relations Theory' in *Oxford Research Encyclopedia of International Studies* (Oxford University Press 2015) ⟨https://perma.cc/V8Q6-DAZD⟩.

Cortell AP and Davis Jr JW, 'Understanding the Domestic Impact of International Norms: A Research Agenda' (2000) 2(1) International Studies Review 65 ⟨https://perma.cc/ERU5-9DLG⟩.

Crawford A, 'Networked Governance and the Post-Regulatory State?' (2006) 10(4) Theoretical Criminology 449 ⟨http://perma.cc/N598-VQ2C⟩.

Crawford K and Lumby C, 'Networks of Governance: Users, Platforms, and the Challenges of Networked Media Regulation' eng (2013) 1(3) International Journal of Technology Policy and Law 270 ⟨http://perma.cc/B2XW-YZHB⟩.

Creswell JW, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (Fourth, SAGE Publications 2013).

Crete-Nishihata M and Deibert RJ, 'Global Governance and the Spread of Cyberspace Controls' (2012) 339(18) Global Governance 339 ⟨https://perma.cc/MEL2-7X6G⟩.

Crowe S and others, 'The Case Study Approach' (2011) 11(1) BMC Medical Research Methodology ⟨https://perma.cc/4JXD-EGCG⟩.

Cutler AC, Haufler V, and Porter T, *Private Authority and International Affairs* (State University of New York Press 1999).

Cyber Law International, Cyber Law International (2020) ⟨https://perma.cc/8VNS-XXRE⟩ accessed 5 September 2020.

CyberPeace Institute, Working Towards a Safer Online World for All (2019) ⟨https://perma.cc/D7VV-JRG5⟩ accessed 17 November 2019.

— Partners (2020) ⟨https://perma.cc/3Y52-TV9D⟩ accessed 6 March 2020.

Cybersecurity Tech Accord, Cybersecurity Tech Accord (2018) ⟨https://perma.cc/4W5G-FK3L⟩ accessed 10 July 2018.

— *2019 Year In Review* (techspace rep, 2019) ⟨https://perma.cc/YX6V-9DLP⟩.

— About the Cybersecurity Tech Accord (2019) ⟨https://perma.cc/6M78-2ZTQ⟩ accessed 19 August 2019.

— Leading by Example: Cybersecurity Tech Accord Welcomes New Signatories and Agrees to Implement Vulnerability Disclosure Policies across the Group (2019) ⟨https://perma.cc/CQJ4-PQDG⟩ accessed 28 August 2020.

— The Cybersecurity Tech Accord Response to a Call for Contributions from Best Practices Forum Working Group on Cybersecurity Culture, Norms and Values (2019) ⟨https://perma.cc/JC8R-VTKK⟩ accessed 28 August 2020.

— The Cybersecurity Tech Accord Welcomes the Global Commission's Singapore Norm Package, Offers Comments on Enhancing Stability in Cyberspace (2019) ⟨https://perma.cc/ZC9T-5FFR⟩ accessed 30 September 2019.

— Policy Submissions (2020) ⟨https://perma.cc/Y7QE-TMPH⟩ accessed 28 August 2020.

— Vulnerability Disclosure Policies (2020) ⟨https://perma.cc/W8H9-DPC2⟩ accessed 28 August 2020.

D'Aspremont J, 'International Law-Making by Non-State Actors: Changing the Model or Putting the Phenomenon into Perspective?' [2010] SSRN Electronic Journal 171 ⟨https://perma.cc/7LSN-2XXX⟩.

— *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law* (D'Aspremont J, Reisman WM, and Noortmann M eds, Routledge Research in International Law, Routledge 2011).

— *Formalism and the Sources of International Law: A Theory of the Ascertainment of Legal Rules* (Oxford University Press 2013).

Daigle L, 30 Years of TCP and IP on Everything (2013) ⟨https://perma.cc/D94R-U79L⟩ accessed 28 February 2018.

Dany C, 'Between Big Deals and Small Steps: Measuring the Effectiveness of International Non-Governmental Organizations' in H Hegemann, R Heller, and M Kahl (eds), *Studying 'Effectiveness' in International Relations: A Guide for Students and Scholars* (Verlag Barbara Budrich 2012).

Deibert RJ, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' (2003) 32(3) Millennium: Journal of International Studies 501 ⟨https://perma.cc/MWB7-W3UU⟩.

Deibert RJ and Rohozinski R, 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4(1) International Political Sociology 15 ⟨https://perma.cc/P58M-ETF7⟩.

Demchak C and Dombrowski P, 'Cyber Westphalia: Asserting State Prerogatives in Cyberspace' [2014] Georgetown Journal of International Affairs 29 ⟨https://perma.cc/79C5-HA6T⟩.

Demidov O and Paoli GP, *Supply Chain Security in the Cyber Age* (techspace rep, United Nations Institute for Disarmament Research 2020) ⟨https://perma.cc/BFQ8-JW3X⟩.

DeNardis L, *The Emerging Field of Internet Governance* (techspace rep, Yale University 2010) ⟨https://perma.cc/Z8VD-7JRZ⟩.

Denzin NK and Lincoln YS, *Strategies of Qualitative Inquiry* (SAGE Publications 2012).

Der Derian J, 'The Question of Information Technology in International Relations' (2003) 32(3) Millennium: Journal of International Studies 441 ⟨https://perma.cc/7QVR-MXMP⟩.

Deutsche Telekom, Teaming Up For More Cybersecurity (2018) ⟨https://perma.cc/ZU9W-EAGH⟩ accessed 28 August 2020.

Devex, Global Partners Digital (2020) ⟨https://perma.cc/267W-R539⟩ accessed 29 August 2020.

Dhillon G and Backhouse J, 'Technical Opinion: Information System Security Management in the New Millennium' (2000) 43(7) Communications of the ACM 125 ⟨https://perma.cc/2U5C-KJEE⟩.

Dobrygowski D, Why Companies Are Forming Cybersecurity Alliances (2019) ⟨https://perma.cc/2NN9-XZ5G⟩ accessed 14 September 2019.

Drake RF, *The Principles of Social Policy* (Palgrave Macmillan UK 2001).

Dubnick MJ and Frederickson HG, *Accountable Governance* (Routledge 2014) ⟨https://perma.cc/GGK3-M8U3⟩.

Dunn Cavelty M, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge 2008).

— 'Cyber-Security and Private Actors', in R Abrahamsen and A Leander (eds), *Routledge Handbook of Private Security Studies* (Routledge 2015) ⟨https://perma.cc/Y47N-DWUE⟩.

Dunn Cavelty M and Eggenschwiler J, Behavioral Norms in Cyberspace: Can Corporations Make the Digital Sphere Secure? (2019) ⟨https://perma.cc/4GQE-EWVR⟩ accessed 10 December 2019.

Dunn Cavelty M and Suter M, 'Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection' (2009) 2(4) International Journal of Critical Infrastructure Protection 179 ⟨https://perma.cc/KK4N-R2SP⟩.

Easterbrook FH, 'Cyberspace and the Law of the Horse' [1996] (1) University of Chicago Legal Forum 207 ⟨https://perma.cc/3TMT-4AZ4⟩.

Easton D, *A Systems Analysis of Political Life* (Wiley 1965).

Eberlein B and others, 'Transnational Business Governance Interactions: Conceptualization and Framework for Analysis' (2014) 8(1) Regulation & Governance 1 ⟨https://perma.cc/U3DH-PCVD⟩.

Efremov A, Ethical Principles for Disclosing Vulnerabilities (2020) ⟨https://perma.cc/3NHY-STM2⟩ accessed 28 August 2020.

Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) American Journal of International Law 583 ⟨https://perma.cc/FSU5-FUJ6⟩.

Eggenschwiler J, 'Accountability Challenges Confronting Cyberspace Governance' (2017) 6(3) Internet Policy Review 1 ⟨https://perma.cc/3KT6-SHGP⟩.

— 'A Typology of Cybersecurity Governance Models' (2018) 13(2) St Antony's International Review 64 ⟨https://perma.cc/4AK4-JGUU⟩.

— *Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector Framework Document* (techspace rep, Geneva Dialogue on Responsible Behaviour in Cyberspace 2018) ⟨https://perma.cc/3WKN-BFH4⟩.

— 'An Incident-Based Conceptualization of Cybersecurity Governance', in R Ellis and VK Mohan (eds), *Rewired: Cybersecurity Governance* (John Wiley & Sons 2019).

— *International Cybersecurity Norm Development: The Roles of States Post-2017* (techspace rep, April, EU Cyber Direct 2019) ⟨https://perma.cc/7PR4-C72T⟩.

— 'Expert Commissions and Norms of Responsible Behaviour in Cyberspace: A Review of the Activities of the GCSC' [2020] Digital Policy, Regulation and Governance ⟨https://perma.cc/4QKH-F2WG⟩.

Eggenschwiler J, Agrafiotis I, and Nurse JR, 'Insider Threat Response and Recovery Strategies in Financial Services Firms' (2016) 2016(11) Computer Fraud & Security 12 ⟨https://perma.cc/L29A-H56C⟩.

Eggenschwiler J and Kulesza J, 'Non-State Actors as Shapers of Customary Standards of Responsible Behaviour in Cyberspace' in D Broeders and B van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020).

Eggenschwiler J and Silomon J, 'Challenges and Opportunities in Cyber Weapon Norm Construction' (2018) 2018(12) Computer Fraud & Security 11 ⟨https://perma.cc/CK9P-CK47⟩.

Egloff FJ, 'Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates' (PhD thesis, University of Oxford 2018) ⟨https://perma.cc/WF6S-YTLR⟩.

Eichensehr KE, 'Review of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)' (2014) 108 American Journal of International Law 585 ⟨https://perma.cc/M8ZG-QS6H⟩.

— 'The Cyber-Law of Nations' (2015) 103(2) Georgetown Law Journal 317 ⟨https://perma.cc/W58Z-SHYU⟩.

— 'Public-Private Cybersecurity' (2017) 95(467) Texas Law Review 16 ⟨https://perma.cc/ZL8H-48JE⟩.

England R, Kaspersky to Move to Switzerland Following Latest Government Ban (2018) ⟨https://perma.cc/UA3C-SWKU⟩ accessed 29 August 2020.

Enjolras B and Sivesind KH, *Civil Society in Comparative Perspective* (Emerald Group Publishing 2009).

Eroukhmanoff C, 'Securitisation Theory' in S McGlinchey, R Walters, and C Scheinpflug (eds), *International Relations Theory* (E-International Relations Publishing 2017) ⟨https://perma.cc/QE6U-CLVC⟩.

Erskine T and Carr M, 'Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace' in A.-M Osula and H Rõigas (eds), *Legal, Policy & Industry Perspectives* (NATO Cooperative Cyber Defence Centre of Excellence 2016) ⟨https://perma.cc/S39A-6786⟩.

EU Cyber Direct, European Union Institute for Security Studies (2020) ⟨https://perma.cc/97DX-DQ99⟩ accessed 29 August 2020.

European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (2013) ⟨https://perma.cc/27F8-5W7J⟩.

— Answer Given by Ms Gabriel on Behalf of the European Commission (2019) ⟨https://perma.cc/C679-GVL2⟩ accessed 29 August 2020.

European Parliament, *Report on Cyber Defence (2018/2004(INI))* (techspace rep, 2018) ⟨https://perma.cc/SLM9-HRVH⟩.

European Union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation' [2019] (L151/15) Official Journal of the European Union 15 ⟨https://perma.cc/6ZG3-SCJW⟩.

European Union Agency for Network and Information Security, *ENISA Good Practice Guide on Vulnerability Disclosure* (techspace rep, November, European Union Agency for Network and Information Security 2015) ⟨https://perma.cc/U5UR-ZYPJ⟩.

Evans G, 'Commission Diplomacy' in AF Cooper, J Heine, and R Thakur (eds), *The Oxford Handbook of Modern Diplomacy* (Oxford University Press 2013) ⟨https://perma.cc/J9QE-CJHJ⟩.

Expert #1, Interview #1 (2019).

Expert #11, Interview #11 (2019).

Expert #12, Interview #12 (2019).

Expert #13, Interview #13 (2019).

Expert #14, Interview #14 (2019).

Expert #16, Interview #16 (2019).

Expert #17, Interview #17 (2019).

Expert #18, Interview #18 (2019).

Expert #19, Interview #19 (2019).

Expert #2, Interview #2 (2019).

Expert #21, Interview #21 (2019).

Expert #22, Interview #22 (2019).

Expert #23, Interview #23 (2019).

Expert #24, Interview #24 (2019).

Expert #25, Interview #25 (2019).

Expert #27, Interview #27 (2019).

Expert #28, Interview #28 (2019).

Expert #29, Interview #29 (2019).

Expert #3, Interview #3 (2019).

Expert #32, Interview #32 (2020).

Expert #4, Interview #4 (2019).

Expert #5, Interview #5 (2019).

Expert #6, Interview #6 (2019).

Expert #9, Interview #9 (2019).

Fairbank NA, 'The State of Microsoft?: The Role of Corporations in International Norm Creation' (2019) 4(3) Journal of Cyber Policy 380 ⟨https://perma.cc/GBZ2-ZAUJ⟩.

Farlex, Diplomatic Agents (2020) ⟨https://perma.cc/J57P-MZGE⟩ accessed 28 August 2020.

Farrell H, *Promoting Norms for Cyberspace* (techspace rep, April, 2015) ⟨https://perma.cc/T9ER-5935⟩.

Ferguson WD, 'Facing Uncertainty: The Role of Norms and Formal Institutions as Shared Mental Models' (SASE Mini-Conference on Uncertain Futures in Economic Decision Making, London, 2019) ⟨https://perma.cc/YFD2-39G3⟩.

Fidler DP, Buchan R, and Crawford E, *Study Group Report* (techspace rep, International Law Association 2016) ⟨https://perma.cc/3GQC-59YZ⟩.

Finnemore M, 'New Directions, New Collaborations for International Law and International Relations' in TJ Biersteker, PJ Spiro, and CL Sriram (eds), *International Law and International Relations* (Routledge 2006).

— 'Cultivating International Cyber Norms', in KM Lord and T Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age* (Center for a New American Security 2011) ⟨https://perma.cc/CBZ2-PHT4⟩.

— 'Cybersecurity and the Concept of Norms' (Carnegie Endowment for International Peace, 2017) ⟨https://perma.cc/K7QA-UL6G⟩.

Finnemore M and Hollis DB, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) The American Journal of International Law 425 ⟨https://perma.cc/QB6N-SZC3⟩.

Finnemore M and Sikkink K, 'International Norm Dynamics and Political Change' (1998) 52(4) International Organization 887 ⟨https://perma.cc/7CWG-H7JE⟩.

Fischerkeller MP and Harknett RJ, 'Deterrence is Not a Credible Strategy for Cyberspace' (2017) 61(3) Orbis 381 ⟨https://perma.cc/B3CL-2TNZ⟩.

Fjeld J and others, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI* (techspace rep, Berkman Klein Center for Internet and Society 2020) ⟨https://perma.cc/8FU2-6J2H⟩.

Flohr A and others, *The Role of Business in Global Governance* (Palgrave Macmillan UK 2010) ⟨https://perma.cc/LN24-QTY3⟩.

— 'Variations in Corporate Norm-Entrepreneurship: Why the Home State Matters', in M Ougaard and A Leander (eds), *Business and Global Governance* (Routledge 2012).

Florini A, 'The Evolution of International Norms' (1996) 40(3) International Studies Quarterly 363 ⟨https://perma.cc/J7ZW-Y3HG⟩.

— *The Third Force: The Rise of Transnational Civil Society* (Ebook central, Japan Center for International Exchange 2000).

Forum of Incident Response and Security Teams, FIRST Announces Incident Response Training for Policymakers (2017) ⟨https://perma.cc/Z5P9-QB5N⟩ accessed 28 August 2020.

— 31st Annual FIRST Conference (2019) ⟨https://perma.cc/QQ7S-WMK2⟩ accessed 28 August 2020.

— Chris Gibson appointed Executive Director at FIRST (2019) ⟨https://perma.cc/N39N-N2VB⟩ accessed 28 August 2020.

— *Position Paper on Cybersecurity Developments Within the UN Context* (techspace rep, Australian Government Department of Foreign Affairs and Trade 2019) ⟨https://perma.cc/33HE-KN3Q⟩.

— About FIRST (2020) ⟨https://perma.cc/3PDT-7NEX⟩ accessed 28 August 2020.

— Board of Directors (2020) ⟨https://perma.cc/RW95-6YDS⟩ accessed 28 August 2020.

— Bylaws of FIRST.Org, Inc. (2020) ⟨https://perma.cc/7WZT-C6S5⟩ accessed 28 August 2020.

— Education (2020) ⟨https://perma.cc/X8S9-8SNF⟩ accessed 28 August 2020.

— Education Programme (2020) ⟨https://perma.cc/AK3A-WNBG⟩ accessed 28 August 2020.

— EthicsfIRST: Ethics for Incident Response and Security Teams (2020) ⟨https://perma.cc/P95R-RQYQ⟩ accessed 28 August 2020.

— FIRST History (2020) ⟨https://perma.cc/LVV9-988R⟩ accessed 28 August 2020.

— FIRST Members (2020) ⟨https://perma.cc/FXG7-ASLE⟩ accessed 28 August 2020.

— FIRST Releases Its 2019-20 Annual Report (2020) ⟨https://perma.cc/B973-H6T2⟩ accessed 28 August 2020.

Forum of Incident Response and Security Teams, Global Initiatives (2020) ⟨https://perma.cc/HYX7-PTZZ⟩ accessed 28 August 2020.

— Mission Statement (2020) ⟨https://perma.cc/X2JR-425Y⟩ accessed 28 August 2020.

— Organisation (2020) ⟨https://perma.cc/H46L-BMEE⟩ accessed 28 August 2020.

— Technical Colloquia & Symposia (2020) ⟨https://perma.cc/KL4G-48D6⟩ accessed 31 August 2020.

— Technical Colloquia & Symposia (2020) ⟨https://perma.cc/698U-GETS⟩ accessed 28 August 2020.

Fouche G and Solsvik T, Aluminum Maker Hydro Battles to Contain Ransomware Attack (2019) ⟨https://perma.cc/R264-TV2U⟩ accessed 2 April 2019.

Frank J, Paris Call: Growing Consensus on Cyberspace (2019) ⟨https://perma.cc/NKG2-ZDP4⟩ accessed 6 March 2020.

Freedom House, *Freedom on the Net 2019: The Crisis of Social Media* (techspace rep, Freedom House 2019) ⟨https://perma.cc/SE35-THYC⟩.

Freedom Online Coalition, Aims and Priorities (2020) ⟨https://perma.cc/D3BA-53K6⟩ accessed 29 August 2020.

Fruhlinger J, What Is Stuxnet, Who Created It and How Does It Work? (2017) ⟨https://perma.cc/4FHJ-S5P9⟩ accessed 4 May 2019.

G20, *Communiqué G20 Finance Ministers and Central Bank Governors Meeting* (techspace rep, G20 2017) ⟨https://perma.cc/M9SC-XFXZ⟩.

Gallie WB, 'Essentially Contested Concepts' (1956) 56 Proceedings of the Aristotelian Society 167 ⟨https://perma.cc/TAX3-PDR3⟩.

Galloway A, Cyber Attacks from State-Based Actor Increasing (2020) ⟨https://perma.cc/3LJK-KD5F⟩ accessed 9 September 2020.

Gartzke E, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth' (2013) 38(2) International Security 41 ⟨https://perma.cc/VS92-3QMS⟩.

Gartzke E and Lindsay JR, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace' (2015) 24(2) Security Studies 316 ⟨https://perma.cc/22M3-W3PJ⟩.

Geneva Dialogue, *Geneva Dialogue Final Report* (techspace rep, 2019).

Geneva Internet Platform Digital Watch, A Rights-Based Approach to Cybersecurity (2017) ⟨https://perma.cc/DF63-9MH5⟩ accessed 4 September 2020.

Gibson W, *Neuromancer* (Berkley Publishing Group 1984).

Giles K and Hagestad II W, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' [2013] 5th International Conference on Cyber Conflict 1 ⟨https://perma.cc/6Q2Z-Y7J2⟩.

Global Commission on Internet Governance, *One Internet* (techspace rep, Centre for International Governance Innovation and Chatham House 2016) ⟨https://perma.cc/GL8F-FFMS⟩.

Global Commission on the Stability of Cyberspace, *Briefings from the Research Advisory Group* (techspace rep, November, 2017) ⟨https://perma.cc/HYQ4-GXSP⟩.

— *Call to Protect the Public Core of the Internet* (techspace rep, November, 2017) ⟨https://perma.cc/XY3H-MB96⟩.

— Call to Protect the Electoral Infrastructure (2018) ⟨https://perma.cc/TX6L-FDMH⟩.

— *GCSC Meeting Singapore: Attendance List* (techspace rep, 2018) ⟨https://perma.cc/G4VF-J8RJ⟩.

— Global Commission Introduces Six Critical Norms Towards Cyber Stability (2018) ⟨https://perma.cc/M43W-8L7R⟩ accessed 5 February 2019.

— Information Sheet (2018) ⟨https://perma.cc/3DEY-6MEP⟩ accessed 4 February 2019.

— *Norm Package Singapore* (techspace rep, 2018) ⟨https://perma.cc/SJB5-5YZP⟩.

— *Advancing Cyberstability* (techspace rep, 2019) ⟨https://perma.cc/7FEY-3VB2⟩.

— *Call for Contributions on the 2019 BPF on Cybersecurity: Submission of the Global Commission on the Stability of Cyberspace* (techspace rep, 2019) ⟨https://perma.cc/M8K8-3VG8⟩.

— European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act (2019) ⟨https://perma.cc/YA4C-L6P5⟩ accessed 25 August 2019.

— *Final Report Fact Sheet* (techspace rep, 2019) ⟨https://perma.cc/TT4W-USKU⟩.

— Global Commission Convenes Fifth Cyber Stability Hearings at the United Nations, Geneva (2019) ⟨https://perma.cc/2ETD-KHQS⟩ accessed 10 February 2019.

— Monthly Update Archives (2019) ⟨https://perma.cc/VWK8-YUUY⟩ accessed 8 December 2019.

— News Archive (2019) ⟨https://perma.cc/BZ8V-JABA⟩ accessed 29 November 2019.

— About (2020) ⟨https://perma.cc/2XFC-5JEJ⟩ accessed 8 January 2020.

Global Forum on Cyber Expertise, Global Partners Digital (2020) ⟨https://perma.cc/8E5Z-BN9Q⟩ accessed 29 August 2020.

Global Partners Digital, GPD Launches New Global Programme to Foster Inclusive Cyber Policy-Making Processes (2016) ⟨https://perma.cc/6CKL-RC7A⟩ accessed 29 August 2020.

— *Framework for Multistakeholder Cyber Policy Development* (techspace rep, Global Partners Digital 2018) ⟨https://perma.cc/88AN-8VNV⟩.

— Cyber Norms in NYC: Takeaways From the OEWG Meeting and UNIDIR Cyber Stability Conference (2019) ⟨https://perma.cc/T5G7-V3SK⟩ accessed 29 August 2020.

— Measures for Stakeholder Engagement in the UN Group of Governmental Experts and Open-Ended Working Group A Global Partners Digital Briefing (2019) ⟨https://perma.cc/6AHQ-FRZ8⟩ accessed 29 August 2020.

— *Our Input to the OEWG Intersessional* (techspace rep, 2019) ⟨https://perma.cc/74KR-Q3KT⟩.

Global Partners Digital, *Our Submission to the Global Commission on the Stability of Cyberspace's Request for Consultation on the Norm Package Singapore* (techspace rep, Global Partners Digital 2019) ⟨https://perma.cc/Q5D4-K5Y5⟩.

— Board of Advisors (2020) ⟨https://perma.cc/6DLL-XQAW⟩ accessed 21 September 2020.

— Cyber Events Calendar (2020) ⟨https://perma.cc/AHS8-947C⟩ accessed 1 September 2020.

— Explore the Issues (2020) ⟨https://perma.cc/XN6S-XJK9⟩ accessed 21 September 2020.

— Financials and Reporting (2020) ⟨https://perma.cc/3S9C-8RWN⟩ accessed 29 August 2020.

— Norms Search Results (2020) ⟨https://perma.cc/9QDS-UCJM⟩ accessed 29 August 2020.

— Our Work (2020) ⟨https://perma.cc/239Q-R7QU⟩ accessed 29 August 2020.

— *Pre-Draft of the OEWG's Report on ICTs* (techspace rep, 2020) ⟨https://perma.cc/T9RU-BHAM⟩.

— Trust and Security (2020) ⟨https://perma.cc/4DH5-2PC5⟩ accessed 29 August 2020.

— Who We Are (2020) ⟨https://perma.cc/Q2TC-LLJC⟩ accessed 29 August 2020.

Goldsmith J, *Cybersecurity Treaties: A Skeptical View* (techspace rep, Hoover Institution 2011) ⟨https://perma.cc/4PYY-HFT9⟩.

Goodin D, Powerful Backdoor Found in Software Used By >100 Banks and Energy Cos. (2017) ⟨https://perma.cc/2CFD-F7FN⟩ accessed 1 April 2020.

Gorwa R and Peez A, 'Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord' [2018] SocArXiv ⟨https://perma.cc/G9TB-QPB2⟩.

— Big Tech Hits the Diplomatic Circuit (2019) ⟨https://perma.cc/BQ82-MWBP⟩ accessed 28 August 2020.

Green JA, 'Introduction' in JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) ⟨https://perma.cc/7VWJ-3PZW⟩.

Greenwald G, Microsoft Handed the NSA Access to Encrypted Messages (2013) ⟨https://perma.cc/28BK-TPUW⟩ accessed 29 February 2020.

Grey DE, *Doing Research in the Real World* (SAGE Publications 2018) ⟨http://perma.cc/Y6PG-VCHY⟩.

Griffiths J, 'What is Legal Pluralism?' (1986) 18(24) Journal of Legal Pluralism and Unofficial Law 1 ⟨https://perma.cc/C5V5-KJN5⟩.

Grigsby A, 'The End of Cyber Norms' (2017) 59(6) Survival 109 ⟨https://perma.cc/Z3EX-FPJS⟩.

— The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased (2018) ⟨https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased⟩ accessed 15 January 2019.

Guest G, Namey EE, and Mithcell ML, 'Qualitative Research: Defining and Designing' in *Collecting Qualitative Data: A Field Manual for Applied Research* (SAGE Publications 2013) ⟨https://perma.cc/W5NS-W8ZV⟩.

Guitton C, *Inside the Enemy's Computer: Identifying Cyber Attackers* (Hurst & Company 2017).

Haas PM, 'Introduction: Epistemic Communities and International Policy Coordination' (1992) 46(1) International Organization 1 ⟨https://perma.cc/M5AD-ZRVT⟩.

Hale T, 'Transnational Actors and Transnational Governance in Global Environmental Politics' (2020) 23 Annual Review of Political Science 203 ⟨https://perma.cc/BV75-C4VL⟩.

Hall RB and Biersteker TJ, *The Emergence of Private Authority in Global Governance* (Cambridge University Press 2002).

Hampson FO and others, *Getting Beyond Norms: New Approaches to International Cyber Security Challenges* (techspace rep, Centre for International Governance Innovation 2017) ⟨https://perma.cc/U8YX-ABDW⟩.

Hansen L and Nissenbaum H, 'Digital Disaster, Cyber Security, and the Copenhagen School' (2009) 53(4) International Studies Quarterly 1155 ⟨https://perma.cc/MQ5B-5WMG⟩.

Hathaway M and Spidalieri F, *The Netherlands Cyber Readiness at a Glance* (techspace rep, Potomac Institute for Policy Studies 2017) ⟨https://perma.cc/DJ5N-5V9N⟩.

Hathaway OA and others, 'The Law of Cyber-Attack' (2012) 100(4) California Law Review 817 ⟨https://perma.cc/642V-LXA3⟩.

Healey J, *Innovation on Cyber Collaboration: Leverage at Scale* (techspace rep, Atlantic Council 2018) ⟨https://perma.cc/ZH4B-8UPY⟩.

Hegemann H, Heller R, and Kahl M, *Studying 'Effectiveness' in International Relations: A Guide for Students and Scholars* (Hegemann H, Heller R, and Kahl M eds, Verlag Barbara Budrich 2012).

Heintschel von Heinegg W, 'The Tallinn Manual and International Cyber Security Law' in *Yearbook of International Humanitarian Law 2012* (Springer 2012).

Henriksen A, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5(1) Journal of Cybersecurity 1 ⟨http://perma.cc/654V-FWKL⟩.

Hern A, Ransomware Attack ot Designed to Make Money, Researchers Claim (2017) ⟨https://perma.cc/6M3N-33XK⟩ accessed 28 May 2018.

— WannaCry, Petya, NotPetya: How Ransomware Hit the Big Tme in 2017 (2017) ⟨https://perma.cc/CNC7-ZSCR⟩.

Herr T, 'PrEP: A Framework for Malware and Cyber Weapons' (2013) 13(1) SSRN Electronic Journal ⟨https://perma.cc/BUM4-7AKB⟩.

— 'Malware Counter-Proliferation and the Wassenaar Arrangement' (IEEE 2016) ⟨https://perma.cc/32GS-JKRR⟩.

Herr T and Rosenzweig P, 'Cyber Weapons and Export Control: Incorporating Dual Use With the Prep Model' (2016) 8(2) Journal of National Security Law and Policy 301 ⟨https://perma.cc/NB6K-4EGL⟩.

Heywood A, *Political Theory: An Introduction* (Heywood A ed, Palgrave Macmillan 2004).

Higgins R, *International Law and How We Use It* (Oxford University Press 1995) ⟨https://perma.cc/C29A-MDLF⟩.

Hinck G, Private-Sector Initiatives for Cyber Norms: A Summary (2018) ⟨https://perma.cc/MR4K-VR4K⟩ accessed 25 June 2018.

Hinkley C, Nation-State Cyberattacks: It's Bigger Than Iran (2020) ⟨https://perma.cc/2EJH-ATQN⟩ accessed 9 September 2020.

Hoffmann MJ, 'Norms and Social Constructivism in International Relations' in *Oxford Research Encyclopaedia of International Studies* (Oxford University Press 2017) ⟨https://perma.cc/DY7C-DU6J⟩.

Hollis DB and Neutze J, 'Defending Democracies via Cybernorms' (Philadelphia, PA, 2020) ⟨https://perma.cc/457E-XQKH⟩.

Homburger Z, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace' (2019) 33(2) Global Society 224.

Horenbeeck MV and others, *Cybersecurity Agreements* (techspace rep, Internet Governance Forum 2019) ⟨http://www.intgovforum.org/multilingual/filedepot_download/4904/1658⟩.

Huelss H, 'After Decision-Making: The Operationalization of Norms in International Relations' (2017) 9(3) International Theory 381.

Hurel LM and Lobato LC, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs' (2018) 3(1) Journal of Cyber Policy 61 ⟨https://perma.cc/F3QL-LKKG⟩.

Hurwitz R, *An Augmented Summary of the Harvard , MIT and University of Toronto Cyber Norms Workshop* (techspace rep, Massachusetts Institute of Technology 2012) ⟨https://perma.cc/QX9P-NFFZ⟩.

— 'The Play of States: Norms and Security in Cyberspace' (2014) 36(5) American Foreign Policy Interests 322 ⟨https://perma.cc/934D-ERHN⟩.

Hyett N, Kenny A, and Dickson-Swift V, 'Methodology or Method a Critical Review of Qualitative Case Study Reports' (2014) 9(1) International Journal of Qualitative Studies on Health and Well-being ⟨https://perma.cc/AEB6-WL4M⟩.

IBM, Charter of Trust Roadshow Brings Top Leaders to DC to Discuss Cybersecurity (2018) ⟨https://perma.cc/HHS3-TPK9⟩ accessed 28 August 2020.

ICT4Peace Foundation, Mission (2020) ⟨https://perma.cc/B6UG-PFSG⟩ accessed 29 August 2020.

Information is Beautiful, World's Biggest Data Breaches & Hacks (2019) ⟨https://perma.cc/K9PT-8S62⟩ accessed 6 December 2019.

Ingber R, 'Interpretation Catalysts in Cyberspace' (2017) 95(7) Texas Law Review 1531 ⟨https://perma.cc/ZLC7-AFSY⟩.

Inkster N, 'Measuring Military Cyber Power' (2017) 59(4) Survival 27 ⟨https://perma.cc/FM48-TGYT⟩.

International Campaign to Abolish Nuclear Weapons, ICAN Receives 2017 Nobel Peace Prize (2017) ⟨https://perma.cc/LR56-TMTF⟩ accessed 6 December 2019.

International Committee of the Red Cross, Geneva Convention (IV) on Civilians, 1949 (2020) ⟨https://perma.cc/ZQ9H-ZKVY⟩ accessed 2 March 2020.

International Organisation for Standardisation, ISO/IEC 27032:2012 (2012) ⟨https://perma.cc/42LC-QM33⟩ accessed 31 March 2019.

International Relations, 'Conversations in International Relations: Interview with John J. Mearsheimer (Part II)' (2006) 20(2) International Relations 231 ⟨https://perma.cc/9F8G-BGDG⟩.

International Telecommunications Union, Definition of Cybersecurity (2008) ⟨https://perma.cc/88DW-9MYA⟩ accessed 8 April 2019.

Jayawardane S, Larik J, and Jackson E, *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance* (techspace rep, The Hague Institute for Global Justice 2015) ⟨https://perma.cc/P9A6-RJ4X⟩.

Jensen ET, 'The Tallinn Manual 2.0: Highlights and Inisghts' (2017) 43(3) Georgetown Journal of International Law 735 ⟨https://perma.cc/S22D-8JZE⟩.

Johnson DR and Post D, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367 ⟨https://perma.cc/PK8M-Z4H2⟩.

Jorgensen DL, 'The Methodology of Participant Observation' in *Participant Observation* (SAGE Publications, Inc 1989).

Josselin D and Wallace W, *Non-State Actors in World Politics* (Josselin D and Wallace W eds, Palgrave Macmillan UK 2001) ⟨https://perma.cc/9KGG-VZ6A⟩.

Kaeser J, Working together for more security in the digital world (2018) ⟨https://perma.cc/U7VN-W9HG⟩ accessed 3 August 2018.

Kaljulaid K, President of the Republic Opening Speech at CyCon 2017 (2017) ⟨https://perma.cc/QYJ3-45P4⟩ accessed 5 June 2020.

— President of the Republic at the Opening of CyCon 2019 (2019) ⟨https://perma.cc/7Y2Z-M6UP⟩ accessed 8 September 2020.

Kaspersky E, Bonjour, Monsieur President! (2019) ⟨https://perma.cc/WD5A-G9XB⟩ accessed 28 August 2020.

Kaspersky Lab, Kaspersky Lab Response to Issuance of DHS Binding Operational Directive 17-01 (2017) ⟨https://perma.cc/YZJ8-WZRQ⟩ accessed 1 April 2020.

— Kaspersky Lab Moving Core Infrastructure from Russia to Switzerland; Opening First Transparency Center (2018) ⟨https://perma.cc/7T4L-VUUK⟩ accessed 29 August 2020.

— Kaspersky Lab's Global Research and Analysis Team Recognized for ShadowPad Discovery (2018) ⟨https://perma.cc/2ZND-HRMC⟩ accessed 31 March 2020.

Kaspersky Lab, Our First Transparency Center Will Be in Switzerland (2018) ⟨https://perma.cc/SM8R-VKMX⟩ accessed 16 May 2018.

— Kaspersky Lab Announces 4% Revenue Growth to $726 million in 2018 (2019) ⟨https://perma.cc/9FJZ-ZHEQ⟩ accessed 17 August 2019.

— Latest News on the Global Transparency Initiative (2019) ⟨https://perma.cc/F826-R4TY⟩ accessed 18 August 2019.

— *Supporting the Fight Against Cybercrime* (techspace rep, 2019) ⟨https://perma.cc/9BD4-R7QU⟩.

— TOP3 Scores (2019) ⟨https://perma.cc/ZQN8-NG9J⟩ accessed 31 March 2020.

— Transparency Centres (2019) ⟨https://perma.cc/F826-R4TY⟩ accessed 18 August 2019.

— Comments on the Initial 'Pre-draft' of the Report of the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security (2020) ⟨https://perma.cc/8LLD-P9YB⟩ accessed 5 April 2020.

— *Cyber Capacity Building Program* (techspace rep, 2020) ⟨https://perma.cc/5LZA-RNCP⟩.

— Kaspersky Relocates Data Processing to Switzerland (2020) ⟨https://perma.cc/EF9V-N2BX⟩ accessed 5 April 2020.

— Kaspersky's Global Transparency Initiative Status Updates (2020) ⟨https://perma.cc/Q47K-HMUS⟩ accessed 2 April 2020.

— Our Principles of Cooperation with Law Enforcement Agencies, Commercial and Public Entities (2020) ⟨https://perma.cc/LF5Z-M73Z⟩ accessed 1 April 2020.

Kaspersky Lab Global Research and Analysis Team, ShadowPad in Corporate Networks (2017) ⟨https://perma.cc/XTT8-RRNJ⟩ accessed 1 April 2020.

Katzenstein PJ, *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press 1996).

Kavanagh C, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century' (Geneva, 2017) ⟨https://perma.cc/ZT92-6GEA⟩.

— 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (August, Washington, DC, 2019) ⟨https://perma.cc/9MCZ-NTQB⟩.

Kavanagh C and Stauffacher D, *A Role for Civil Society in Cybersecurity Affairs* (techspace rep, ICT4Peace Foundation 2014) ⟨https://perma.cc/57TS-WEG9⟩.

Kazakova A, Enhance Trust in Cyberspace Through the Paris Call (2019) ⟨https://perma.cc/26QH-LQ7Y⟩ accessed 28 August 2020.

Kazakova A and Dechoux A, Working Together to Ensure Trust in and the Security of Cyberspace: Our Contribution to the Paris Call Consultation (2020) ⟨https://perma.cc/5LZS-45YU⟩ accessed 28 August 2020.

Keck ME and Sikkink K, 'Transnational Advocacy Networks in International and Regional Politics' (1999) 51(159) International Social Science Journal 89 ⟨https://perma.cc/FR9H-ZFBR⟩.

Kello L, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' (2013) 38(2) International Security 7 ⟨https://perma.cc/2CSB-58RZ⟩.

— *The Virtual Weapon and International Order* (Yale University Press 2017) ⟨https://perma.cc/T2T6-ZFHD⟩.

Keohane RO and Nye JSJ, *Power and Independence* (Little, Brown and Company 1977).

Kilovaty I, 'Privatized Cybersecurity Law' UC Irvine Law Review ⟨https://perma.cc/UBR6-SVZ8⟩.

Kim E, Microsoft Has a Strange New Mission Statement (2015) ⟨https://perma.cc/Y4AN-LNN8⟩ accessed 27 February 2020.

Kissel RL, *Glossary of Key Information Security Terms* (techspace rep, National Institute of Standards and Technology 2013) ⟨https://perma.cc/2WPU-LMU3⟩.

Kleinwächter W, The Kaljurand Commission: Building Bridges Over Troubled Cyber-Water (2017) ⟨https://perma.cc/VC97-F5V8⟩ accessed 23 April 2018.

— *Towards a Holistic Approach for Internet Related Public Policy Making* (techspace rep, Global Commission on the Stability of Cyberspace 2018) ⟨https://perma.cc/9MJU-GDGC⟩.

Klimburg A, 'Mobilising Cyber Power' (2011) 53(1) Survival 41 ⟨https://perma.cc/8ZNN-AEBQ⟩.

Koederitz M, Strengthening the Charter of Trust for a Secure Digital World (2018) ⟨https://perma.cc/WC7E-FAJ9⟩ accessed 28 August 2020.

Koh HH, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal Online 2 ⟨https://perma.cc/B7TJ-55U5⟩.

Köhn R, Daimler Verlässt Allianz Gegen Cyberattacken (2020) ⟨https://perma.cc/8DCD-WX27⟩ accessed 31 March 2020.

Koppell JG, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"' (2005) 65(1) Public Administration Review 94 ⟨https://perma.cc/Q86G-YVYS⟩.

Kornprobst M, 'Non-State Actors in International Relations: Actors, Processes, and an Agenda for Multifaceted Dialogue' in *Non-State Actors in International Law* (Hart Publishing 2015) ⟨https://perma.cc/22N2-K8MB⟩.

Kramer FD, 'Cyberpower and National Security: Policy Recommendations for a Strategic Framework' in FD Kramer, SH Starr, and LK Wentz (eds), *Cyberpower and National Security* (National Defense University Series, Potomac Books Inc 2009).

Krasner SD, *International Regimes* (Cornell University Press 1983).

Kratochwil F, 'The Force of Prescriptions' (1984) 38(4) International Organization 685 ⟨https://perma.cc/KPH5-G5WZ⟩.

Kratochwil F and Ruggie JG, 'International Organization Foundation International Organization: A State of the Art on an Art of the State' (1986) 40(4) International Organization 753 ⟨https://perma.cc/M5ZX-N7UJ⟩.

Kremer J.-F and Müller B, *Cyberspace and International Relations* (Kremer J.-F and Müller B eds, Springer Berlin Heidelberg 2014) ⟨https://perma.cc/6Y94-7WY7⟩.

Kriesi H, *New Social Movements in Western Europe: A Comparative Analysis* (University of Minnesota Press 1995).

Kruck A and Schneiker A, *Researching Non-State Actors in International Security: Theory and Practice* (Routledge Critical Security Studies, Routledge 2017).

Kuehl DT, 'From Cyberspace to Cyberpower: Defining the Problem' in FD Kramer, SH Starr, and LK Wentz (eds), *Cyberpower and National Security* (Potomac Books Inc 2009).

Kurowska X, *The Politics of Cyber Norms: Beyond Norm Construction* (techspace rep, EU Cyber Direct 2019) ⟨https://perma.cc/B67N-JM2T⟩.

Kusters K and others, 'Participatory Planning, Monitoring and Evaluation of Multi-Stakeholder Platforms in Integrated Landscape Initiatives' (2018) 62(1) Environmental Management 170 ⟨https://perma.cc/Z3XT-GUHF⟩.

Laksmana E, Realism and Non-State Actors Revisited (2013) ⟨https://perma.cc/2NN9-N3G6⟩ accessed 16 July 2019.

Langner R, 'Stuxnet: Dissecting a Cyberwarfare Weapon' (2011) 9(3) IEEE Security & Privacy Magazine 49 ⟨https://perma.cc/EVQ6-AC7Y⟩.

— *To Kill a Centrifuge* (techspace rep, The Langner Group 2013) ⟨https://perma.cc/J3BC-6UN7⟩.

Laudrain APB, Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace (2018) ⟨https://perma.cc/DD7J-JGQF⟩ accessed 5 December 2018.

Legros S and Cislaghi B, 'Mapping the Social-Norms Literature: An Overview of Reviews' (2020) 15(1) Perspectives on Psychological Science 62 ⟨https://perma.cc/UG57-JEHT⟩.

Leiden University, The Hague Program for Cyber Norms (2020) ⟨https://perma.cc/D9M6-ZC6B⟩ accessed 29 August 2020.

Leiner BM and others, 'A Brief History of the Internet' (2009) 39(5) ACM SIGCOMM Computer Communication Review 22 ⟨https://perma.cc/KR8K-6KR4⟩.

Lessig L, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books 2006).

Levers M.-JD, 'Philosophical Paradigms, Grounded Theory, and Perspectives on Emergence' (2013) 3(4) SAGE Open ⟨https://perma.cc/8894-8MAW⟩.

Levy I, Managing Supply Chain Risk in Cloud-Enabled Products (2017) ⟨https://perma.cc/SN2G-4NM9⟩ accessed 29 August 2020.

Levy JS, 'Qualitative Methods and Cross-Method Dialogue in Political Science' (2007) 40(2) Comparative Political Studies 196 ⟨https://perma.cc/QX6S-MGBT⟩.

Lewis J, *Economic Impact of Cybercrime – No Slowing Down* (techspace rep, McAfee 2018) ⟨https://perma.cc/J987-TUS8⟩.

Lewis JA, UN Publishes Latest Report of the Group of Government Experts (2015) ⟨https://perma.cc/V5WD-DPDN⟩ accessed 21 August 2018.

Libicki MC, *Cyberdeterrence and Cyberwar* (RAND Corporation 2009).

Lin H, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (Aegis Paper Series No. 1607, 2016).

Lindsay JR, 'Stuxnet and the Limits of Cyber Warfare' (2013) 22(3) Security Studies 365 ⟨https://perma.cc/2X63-UJ9K⟩.

— 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack' (2015) 1(1) Journal of Cybersecurity 53 ⟨https://perma.cc/QZ7B-WQEU⟩.

Lotrionte C, 'Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law' (2018) 3(2) The Cyber Defense Review 73 ⟨https://perma.cc/8VTM-CMCJ⟩.

Mabry L, 'Case Study in Social Research' in *The SAGE Handbook of Social Research Methods* (SAGE Publications, Ltd 2008).

Mačák K, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) 30(4) Leiden Journal of International Law 877 ⟨https://perma.cc/498K-JFJV⟩.

— 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 American Journal of International Law 81.

Malcolm J, 'Criteria of Meaningful Stakeholder Inclusion in Internet Governance' (2015) 4(4) Internet Policy Review ⟨https://perma.cc/56TW-HNGQ⟩.

Manyika J and Roxburgh C, *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity* (techspace rep, McKinsey & Company 2011) ⟨https://perma.cc/PUB4-EVB9⟩.

Maoz Z, 'Case Study Methodology in International Studies: From Storytelling to Hypothesis Testing' in M Brecher and FP Harvey (eds), *Millennial Reflections on International Studies* (University of Michigan Press 2002).

Marchetti R, Global Civil Society (2016) ⟨https://perma.cc/69H6-WEB8⟩ accessed 6 May 2020.

Matsakis L, The US Sits Out an International Cybersecurity Agreement (2018) ⟨https://perma.cc/6F5B-V24W⟩ accessed 13 December 2018.

Maurer T, *Cyber Norm Emergence at the United Nations* (techspace rep, September, The Belfer Center for Science and International Affairs 2011) ⟨https://perma.cc/6SNR-5DX9⟩.

— *Cyber Mercenaries* (Cambridge University Press 2018).

— 'A Dose of Realism: The Contestation and Politics of Cyber Norms' [2019] Hague Journal on the Rule of Law ⟨https://perma.cc/47E3-8VH7⟩.

Maurer T, Levite A, and Perkovich G, 'Toward a Global Norm Against Manipulating the Integrity of Financial Data' (Washington, DC, 2017) ⟨https://perma.cc/SMH6-WWT7⟩.

Maurer T and Morgus R, *Compilation of Existing Cybersecurity and Information Security Related Definitions* (techspace rep, New America 2014) ⟨https://perma.cc/PWD7-HKLY⟩.

— 'Cybersecurity' and Why Definitions Are Risky (2014) ⟨https://perma.cc/ZC3R-4P34⟩ accessed 11 April 2019.

Mazanec BM, 'Conclusions and Recommendations' in *The Evolution of Cyber War* (University of Nebraska Press 2015).

Mazanec BM, 'Constraining Norms for Cyber Warfare Are Unlikely' (2016) 17(3) Georgetown Journal of International Affairs 100 ⟨https://perma.cc/DC74-BH33⟩.

McBarnet D and Whelan C, 'The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control' (1991) 54(6) The Modern Law Review 848 ⟨https://perma.cc/X49D-94KH⟩.

McConnell M, 'Cyberwar Is the New Atomic Age' (2009) 26(3) New Perspectives Quarterly 72 ⟨https://perma.cc/XSQ6-RS36⟩.

McGann JG, *Democratization and Market Reform in Developing and Transitional Countries: Think Tanks as Catalysts* (Routledge research in comparative politics, Routledge 2010).

— *2019 Global Go To Think Tank Index Report* (techspace rep, University of Pennsylvania 2019) ⟨https://perma.cc/52T5-EFJF⟩.

— *Think Tanks, Foreign Policy and the Emerging Powers* (McGann JG ed, Springer International Publishing 2019) ⟨https://perma.cc/Z9UL-U4S4⟩.

Mearsheimer JJ, 'The False Promise of International Institutions' (1994) 19(3) International Security 5 ⟨https://perma.cc/3K2C-PB4S⟩.

Meridian, About Meridian (2020) ⟨https://perma.cc/FQ3A-KQCN⟩ accessed 28 August 2020.

Meyer M, 'The Rise of the Knowledge Broker' (2010) 32(1) Science Communication 118 ⟨https://perma.cc/2Z6Z-22R3⟩.

Microsoft, *Five Principles for Shaping Cybersecurity Norms* (techspace rep, Microsoft 2013) ⟨https://perma.cc/G6RJ-883W⟩.

— *A Digital Geneva Convention to Protect Cyberspace* (techspace rep, Microsoft Policy Papers 2017) ⟨https://perma.cc/698H-84P5⟩.

— Digital Peace Now (2018) ⟨https://perma.cc/88RC-N8ZX⟩ accessed 4 December 2018.

— *Microsoft 2019 Annual Report* (techspace rep, 2019) ⟨https://perma.cc/55GR-AFDD⟩.

— Facts About Microsoft (2020) ⟨https://perma.cc/TQT2-9KFT⟩ accessed 27 February 2020.

Miller M, Microsoft, Mastercard, Hewlett Foundation Launch Institute to Investigate Cyberattacks (2019) ⟨https://perma.cc/X827-S4DG⟩ accessed 6 March 2020.

Minárik T and Meij K van der, Geneva Conventions Apply to Cyberspace: No Need for a Digital Geneva Convention (2017) ⟨https://perma.cc/PR4J-P3CV⟩ accessed 2 March 2020.

Ministère de l'Europe et des Affaires Étrangères, Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace (2018) ⟨https://perma.cc/8P82-X5JU⟩ accessed 10 December 2018.

Ministère des Armées, *International Law Applied to Operations in Cyberspace* (techspace rep, 2019) ⟨https://perma.cc/K65Z-9E8V⟩.

Ministry of Foreign Affairs of the Netherlands, Letter to the Parliament on the International Legal Order in Cyberspace (2019) ⟨https://perma.cc/Q7D5-XUCZ⟩ accessed 29 August 2020.

Ministry of Foreign Affairs of the Russian Federation, Concept of the Foreign Policy of the Russian Federation (Unofficial Translation) (2013) ⟨https://perma.cc/3S6D-9AS4⟩ accessed 13 April 2019.

MITRE Corporation, Community of Interest and/or Community of Practice (2016) ⟨https://perma.cc/4LWR-HXYT⟩ accessed 8 January 2021.

Moore S and Keen E, Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 (2018) ⟨https://perma.cc/8W6J-FWH8⟩ accessed 3 April 2019.

Moravcsik A, 'Taking Preferences Seriously: A Liberal Theory of International Politics' (1997) 51(4) International Organization 513 ⟨https://perma.cc/J8W8-6ZRL⟩.

Morgan SJ and others, 'Case Study Observational Research: A Framework for Conducting Case Study Research Where Observation Data Are the Focus' (2017) 27(7) Qualitative Health Research 1060 ⟨https://perma.cc/5SPT-XSA6⟩.

Moynihan H, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace' [2020] Journal of Cyber Policy 1 ⟨https://perma.cc/94ZW-86WT⟩.

Muller LP, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities* (techspace rep, Norwegian Institute of International Affairs 2015) ⟨https://perma.cc/KNY9-DXU8⟩.

Munich Security Conference, *Munich Security Report 2018* (techspace rep, Munich Security Conference 2018) ⟨https://perma.cc/4V6C-M6Z5⟩.

Murphy H and Kellow A, 'Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas' (2013) 4(2) Global Policy 139 ⟨https://perma.cc/3E75-TD8G⟩.

Murray A, *Information Technology Law: The Law and Society* (Oxford University Press 2013).

Nasiritousi N, *Shapers, Brokers and Doers: The Dynamic Roles of Non-State Actors in Global Climate Change Governance* (Linköping University 2016) ⟨https://perma.cc/D892-CQQ2⟩.

Nasiritousi N, Hjerpe M, and Linnér B, 'The Roles of Non-State Actors in Climate Change Governance: Understanding Agency Through Governance Profiles' (2016) 16(1) International Environmental Agreements: Politics, Law and Economics 109 ⟨https://perma.cc/P4EB-WSFT⟩.

NATO Cooperative Cyber Defence Centre of Excellence, United Nations Group of Governmental Experts' Long-Awaited Report on Maintaining Peace and Stability of the ICT Environment (2013) ⟨https://perma.cc/86B7-6KYL⟩ accessed 18 January 2019.

— 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law (2015) ⟨https://perma.cc/9558-MZ42⟩ accessed 18 January 2019.

— Strategy and Governance (2019) ⟨https://perma.cc/LQ65-3TZN⟩ accessed 11 April 2019.

Naughton J, 'The Evolution of the Internet: From Military Experiment to General Purpose Technology' (2016) 1(1) Journal of Cyber Policy 5 ⟨https://perma.cc/E92M-XEJZ⟩.

Newton C, The Verge Tech Survey 2020 (2020) ⟨https://perma.cc/DJ95-56SL⟩ accessed 28 August 2020.

Nicholas P, Filling the Gaps in International Law Is Essential to Making Cyberspace a Safer Place (2018) ⟨https://perma.cc/MS7P-2FLL⟩ accessed 28 August 2020.

Noortmann M, 'Understanding Non-State Actors in the Contemporary World Society: Transcending the International, Mainstreaming the Transnational, or Bringing the Participants Back In?' in C Ryngaert and M Noortmann (eds), *Non-State Actor Dynamics in International Law* (Routledge 2016) ⟨https://perma.cc/S825-KPCZ⟩.

Noortmann M, Reinisch A, and Ryngaert C, *Non-State Actors in International Law* (Noortmann M, Reinisch A, and Ryngaert C eds, Studies in International Law, Hart Publishing 2015).

Noortmann M and Ryngaert C, *Non-State Actor Dynamics in International Law: From Law-Takers to Law-Makers* (Noortmann M and Ryngaert C eds, Routledge 2016).

Noortmann M, Ryngaert C, and Reinisch A, 'Introduction' in *Non-State Actors in International Law* (Hart Publishing 2015) ⟨https://perma.cc/3CLG-ZNM5⟩.

Nowell LS and others, 'Thematic Analysis' (2017) 16(1) International Journal of Qualitative Methods ⟨https://perma.cc/567A-KUU7⟩.

NTT, NTT Signed 10 Principles of the Charter of Trust (CoT) (2020) ⟨https://perma.cc/3DCL-6MUT⟩ accessed 28 August 2020.

NXP, NXP and Partners Sign Joint Charter on Cybersecurity (2018) ⟨https://perma.cc/XRD5-VDAF⟩ accessed 28 August 2020.

Nye JSJ, 'Cyber Power' [2010] (May) Belfer Center for Science and International Affairs 1 ⟨https://perma.cc/GHB4-63ED⟩.

— 'Nuclear Lessons for Cyber Security?' (2011) 5(4) Strategic Studies Quarterly 18 ⟨https://perma.cc/BUA8-GSMA⟩.

— *The Future of Power: Its Changing Nature and Use in the Twenty-First Century* (PublicAffairs 2011).

— 'The Regime Complex for Managing Global Cyber Activities' (Paper Series, Centre for International Governance Innovation and Chatham House 2014) ⟨https://perma.cc/3L4P-Z2LP⟩.

Nye JSJ, A Normative Approach to Preventing Cyberwarfare (2017) ⟨https://perma.cc/D2E3-UDJL⟩ accessed 10 November 2017.

— How Will New Cybersecurity Norms Develop? (2018) ⟨https://perma.cc/9NLG-HZJC⟩ accessed 31 May 2018.

— 'Normative Restraints on Cyber Conflict' (Cambridge, MA, 2018) ⟨https://perma.cc/7TS9-CG8G⟩.

— Eight Norms for Stability in Cyberspace (2019) ⟨https://perma.cc/M2DP-SQ6M⟩ accessed 6 December 2019.

Nye JSJ and Donahue JD, *Governance in a Globalizing World* (Brookings Institution Press 2000).

Office of Management and Budget, *An American Budget, Fiscal Year 2019* (techspace rep, 2018) ⟨https://perma.cc/4EJA-9N49⟩.

Olmstead K and Smith A, *Americans and Cybersecurity* (techspace rep, Pew Research Center 2017) ⟨https://perma.cc/P55P-SR7R⟩.

Olsen M, Schneier B, and Zittrain J, *Don't Panic* (techspace rep, Berkman Klein Center for Internet & Society 2016) ⟨https://perma.cc/4ZFT-55C4⟩.

Onuf NG, *World of Our Making: Rules and Rule in Social Theory and International Relations* (University of South Carolina Press 1989).

Osborne C, ShadowPad: Backdoor in Enterprise Server Software Exposed (2017) ⟨https://perma.cc/9QTN-B4VK⟩ accessed 31 March 2020.

Painter C, *Deterrence in Cyberspace* (techspace rep, Australian Strategic Policy Institute Limited 2018) ⟨https://perma.cc/H9XT-TBM9⟩.

Papadopoulos Y, 'Cooperative Forms of Governance: Problems of Democratic Accountability in Complex Environments' (2003) 42(4) European Journal of Political Research 473 ⟨https://perma.cc/R2FE-2GVP⟩.

— 'Accountability and Multi-level Governance: More Accountability, Less Democracy?' (2010) 33(5) West European Politics 1030 ⟨https://perma.cc/DP8Q-8VXF⟩.

Paris Call for Trust and Security in Cyberspace, Paris Call for Trust and Security in Cyberspace (2019) ⟨https://perma.cc/5XSD-5HGV⟩ accessed 5 March 2020.

Parker C, 'The Pluralization of Regulation' (2008) 9(2) Theoretical Inquiries in Law ⟨http://perma.cc/RX3H-52RL⟩.

Parker DB, *Fighting Computer Crime: A New Framework for Protecting Information* (J Wiley 1998).

Patton MQ, *Qualitative Evaluation and Research Methods* (SAGE Publications 2002) ⟨https://perma.cc/WKY9-FZ95⟩.

Pawlak P, *Riding the Digital Wave* (techspace rep, European Union Institute for Security Studies 2014) vol 21 ⟨https://perma.cc/FLP4-KTM4⟩.

Peters A, Closing the Global Cyber Enforcement Gap (2018) ⟨https://perma.cc/AHB2-CWVA⟩ accessed 19 December 2018.

Peters A, Förster T, and Koechlin L, *Towards Non-State Actors as Effective, Legitimate, and Accountable Standard Setters* (Peters A and others eds, Cambridge University Press 2009) ⟨https://perma.cc/44ZV-ACEA⟩.

Peters A, Koechlin L, and Zinkernagel GF, 'Non-State Actors as Standard Setters: Framing the Issue in an Interdisciplinary Fashion' in A Peters and others (eds), *Non-State Actors as Standard Setters* (Cambridge University Press 2009) ⟨https://perma.cc/U5J2-8B3J⟩.

Pfleeger SL and Pfleeger CP, *Security in Computing, Third Edition* (3rd, Prentice Hall 2002).

Pollard A and Court J, 'How Civil Society Organisations Use Evidence to Influence Policy Processes: A Literature Review' (London, 2005) ⟨https://perma.cc/7K3V-9KBG⟩.

QSR International, What is NVivo? (2017) ⟨https://perma.cc/7KDY-FLD5⟩.

Quarmby S, Evidence-Informed Policymaking: Does Knowledge Brokering Work? (2018) ⟨https://perma.cc/YX5J-BQDB⟩ accessed 29 August 2020.

Radin A and Reach C, *Russian Views of the International Order* (techspace rep, RAND Corporation 2017) ⟨https://perma.cc/9QSX-NRAR⟩.

Radu R, 'Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace' in J.-F Kremer and B Müller (eds), *Cyberspace and International Relations* (Springer Berlin Heidelberg 2014) ⟨https://perma.cc/SQ6Z-PVTC⟩.

Ratnesar R, Microsoft's Brad Smith Wants to Restore Trust in Big Tech (2019) ⟨https://perma.cc/JYB5-S6W4⟩ accessed 16 September 2019.

Raustiala K and Slaughter A.-M, 'International Law, International Relations and Compliance' in *Handbook of International Relations* (SAGE Publications 2012) ⟨https://perma.cc/G54M-ZTZH⟩.

Raymond M, 'Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot' [2016] Strategic Studies Quarterly 123 ⟨https://perma.cc/K39C-PDSB⟩.

Raymond M and DeNardis L, 'Multistakeholderism: Anatomy of an Inchoate Global Institution' (2015) 7(3) International Theory 572 ⟨https://perma.cc/L5AK-ZTP2⟩.

Reidenberg JR, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76(3) Texas Law Review 553 ⟨https://perma.cc/WPX4-6BBE⟩.

Reinalda B, 'Non-State Actors in the International System of States' in *The Ashgate Research Companion to Non-State Actors* (Routledge 2016).

Reuters, Microsoft Corporation Profile (2020) ⟨https://perma.cc/QZ4E-9CVA⟩ accessed 27 February 2020.

Rid T, 'Cyber War Will Not Take Place' (2012) 35(1) Journal of Strategic Studies 5 ⟨https://perma.cc/Q54H-PP5G⟩.

Rid T and Arquilla J, 'Think Again: Cyberwar' [2012] (192) Foreign Policy 80 ⟨https://perma.cc/9CBL-NUTJ⟩.

Rid T and Buchanan B, 'Attributing Cyber Attacks' (2015) 38(1-2) Journal of Strategic Studies 4 ⟨https://perma.cc/EV3G-NSEH⟩.

Rid T and McBurney P, 'Cyber-Weapons' (2012) 157(1) The RUSI Journal 6 ⟨https://perma.cc/JT6T-PHUD⟩.

Risse-Kappen T, *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures and International Institutions* (Cambridge Studies in International Relations, Cambridge University Press 1995).

Risse-Kappen T, Ropp SC, and Sikkink K, *The Power of Human Rights: International Norms and Domestic Change* (Cambridge Studies in International Relations, Cambridge University Press 1999).

Ruggie JG, 'Territoriality and Beyond: Problematizing Modernity in International Relations' (1993) 47(1) International Organization 139 ⟨https://perma.cc/DQR5-ZBTB⟩.

— 'Reconstituting the Global Public Domain - Issues, Actors, and Practices' (2004) 10(4) European Journal of International Relations 499 ⟨https://perma.cc/W6T5-BATR⟩.

— *The Social Construction of the UN Guiding Principles on Business and Human Rights* (techspace rep, Harvard Kennedy School 2017) ⟨https://perma.cc/F3QN-VPTB⟩.

Ruhl C and others, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (techspace rep, February, Carnegie Endowment for International Peace 2020) ⟨https://perma.cc/WXC3-JAEP⟩.

Ryan JJCH, Ryan DJ, and Tikk E, *Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation* (techspace rep, 2010) ⟨https://perma.cc/KCJ8-G3ZS⟩.

Salkind N, *Encyclopedia of Research Design* (SAGE Publications 2010) ⟨https://perma.cc/U6BV-FKNB⟩.

Sandholtz W, *International Norm Change* (Oxford University Press 2017) ⟨https://perma.cc/8629-CB4Z⟩.

Sayers R, *Principles of Awareness-Raising: Information Literacy, a Case Study* (techspace rep, UNESCO 2006) ⟨https://perma.cc/L5XC-SKAV⟩.

Schensul SL, Schensul JJ, and LeCompte MD, *Essential Ethnographic Methods: Observations, Interviews, and Questionnaires* (Altamira Press 1999).

Schia NN, 'The Cyber Frontier and Digital Pitfalls in the Global South' (2018) 39(5) Third World Quarterly 821 ⟨https://perma.cc/3UW7-XLM3⟩.

Schmitt M and Vihul L, International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms (2017) ⟨https://perma.cc/ALK4-EGDN⟩ accessed 5 September 2020.

Schmitt MN, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt MN ed, Cambridge University Press 2013) ⟨https://perma.cc/A829-LAC8⟩.

— Factsheet: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017) ⟨https://perma.cc/7WD2-NNX6⟩ accessed 27 March 2018.

Schmitt MN, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum' (2017) 8 Harvard National Security Journal ⟨https://perma.cc/5GVK-NLT6⟩.

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt MN ed, Cambridge University Press 2017) ⟨https://perma.cc/C42C-QVVE⟩.

Schmitt MN, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty' (2019) 126 Harvard Law Review Forum 176 ⟨https://perma.cc/82FR-TA6Z⟩.

— The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis (2019) ⟨https://perma.cc/6AN7-BKN6⟩ accessed 29 August 2020.

Schmitt MN and Vihul L, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) 1(2) Fletcher Security Review 55 ⟨https://perma.cc/6XZQ-K8M2k⟩.

Scholte JA, 'Global Civil Society: Changing the World?' (Warwick, 1999) ⟨https://perma.cc/QJ2G-R7V5⟩.

— *Building Global Democracy?* (Scholte JA ed, Cambridge University Press 2011).

Shachtman N, Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals (2012) ⟨https://perma.cc/P7YG-JFRL⟩ accessed 1 April 2020.

Shackelford SJ, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press 2014).

Shany Y, 'Assessing the Effectiveness of International Courts: A Goal-Based Approach' (2012) 106(2) The American Journal of International Law 225 ⟨https://perma.cc/X9YF-MYWT⟩.

Shires J and Smeets M, 'What Do We Talk About When We Talk About Cyber?' [2016] SSRN Electronic Journal ⟨https://perma.cc/UD9S-D645⟩.

Shor E, 'Conflict, Terrorism, and the Socialization of Human Rights Norms: The Spiral Model Revisited' (2008) 55(1) Social Problems 117 ⟨https://perma.cc/CTW3-J73T⟩.

Siemens, *Siemens Annual Report 2018* (techspace rep, 2018).

— *Annual Report 2019* (techspace rep, 2019) ⟨https://perma.cc/GFU3-J558⟩.

— Charter of Trust on Cybersecurity (2019) ⟨https://perma.cc/P2M9-EE62⟩ accessed 1 March 2020.

— One Year Charter of Trust: Important Milestones for More Cybersecurity (2019) ⟨https://perma.cc/8CTL-NEQD⟩ accessed 16 September 2019.

— The Charter of Trust Takes a Major Step Forward to Advance Cybersecurity (2019) ⟨https://perma.cc/MU7Q-G784⟩.

— About Us (2020) ⟨https://perma.cc/3EPV-4TF3⟩ accessed 9 March 2020.

— Charter of Trust Partners Decide on Further Measures for More Cybersecurity (2020) ⟨https://perma.cc/23N3-VNKC⟩ accessed 25 March 2020.

— Security Settings in WinCC (2020) ⟨https://perma.cc/U8B4-TUX2⟩ accessed 28 August 2020.

Sigholm J, 'Non-State Actors in Cyberspace Operations' (2013) 4(1) Journal of Military Studies 1 ⟨https://perma.cc/7EKB-UZR9⟩.

Singer PW and Friedman A, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014).

Skierka I and others, 'CSIRT Basics for Policy-Makers' (Washington, DC and Berlin, 2015) ⟨https://perma.cc/7JRM-P5M9⟩.

Slack C, 'Wired Yet Disconnected: The Governance of International Cyber Relations' (2016) 7(1) Global Policy 69 ⟨https://perma.cc/N882-S5QJ⟩.

— 'Wired yet Disconnected: The Governance of International Cyber Relations' (2016) 7(1) Global Policy 69 ⟨https://perma.cc/KR29-XE9X⟩.

Slaughter A.-M, 'International Relations, Principal Theories' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2011).

— 'International Law and International Relations Theory: Twenty Years Later', in JL Dunoff and MA Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (2012).

Slaughter A.-M, Tulumello AS, and Wood S, 'International Law and International Relations Theory: A New Generation of Interdisciplinary Scholarship' (1998) 92(3) The American Journal of International Law 367 ⟨https://perma.cc/F5Y6-92Z7⟩.

Smeets M, 'A Matter of Time: On the Transitory Nature of Cyberweapons' (2018) 41(1-2) Journal of Strategic Studies 6 ⟨https://perma.cc/6WV2-V7G5⟩.

Smith B, The Need For a Digital Convention (2017) ⟨https://perma.cc/4J63-P45T⟩ accessed 9 July 2018.

— 34 Companies Stand Up for Cybersecurity with a Tech Accord (2018) ⟨https://perma.cc/J3MH-559K⟩ accessed 10 July 2018.

— An Important Step Toward Peace and Security in the Digital World (2018) ⟨https://perma.cc/25C9-2C82⟩ accessed 4 March 2020.

Spiegel R, Siemens Pushes Cybersecurity to the Highest Levels (2018) ⟨https://perma.cc/4TPX-6RQV⟩ accessed 28 August 2020.

Spiro PJ, 'Nongovernmental Organizations in International Relations (Theory)' in JL Dunoff and MA Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations* (Cambridge University Press 2012).

Stake RE, 'Qualitative Case Studies' in NK Denzin and YS Lincoln (eds), *The SAGE Handbook of Qualitative Research* (Sage 2005).

Stevens T, Cyberweapons: Governing the Ungovernable? (2016) ⟨https://perma.cc/4R7C-9REX⟩ accessed 30 November 2019.

— 'Cyberweapons: Power and the Governance of the Invisible' (2017) 55(3-4) International Politics 482 ⟨https://perma.cc/7S5A-BXXX⟩.

Stiles K and Sandholtz W, 'Cycles of International Norm Change' in K Stiles and W Sandholtz (eds), *International Norms and Cycles of Change* (Oxford University Press 2008).

Stone J, 'Cyber War Will Take Place!' (2013) 36(1) Journal of Strategic Studies 101 ⟨https://perma.cc/43E6-XLAV⟩.

Suchman MC, 'Managing Legitimacy: Strategic and Institutional Approaches' (1995) 20(3) The Academy of Management Review 571 ⟨https://perma.cc/A2CW-DMQR⟩.

Suter WN, 'Qualitative Data, Analysis, and Design' in *Introduction to Educational Research: A Critical Thinking Approach* (SAGE Publications 2014).

Suzor N, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) Social Media Society 1 ⟨https://perma.cc/972B-TAM7⟩.

Tamanaha BZ, 'The Folly of the 'Social Scientific' Concept of Legal Pluralism' (1993) 20(2) Journal of Law and Society 192 ⟨https://perma.cc/9YL7-DAAL⟩.

Tanczer LM, Brass I, and Carr M, 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy' (2018) 9(3) Global Policy 60 ⟨https://perma.cc/KV4X-6LMM⟩.

The Economist, The World's Most Valuable Resource Is No Longer Oil, But Data (2017) ⟨https://perma.cc/MAZ9-QY4L⟩ accessed 21 May 2019.

The Guardian, The NSA Files (2013) ⟨https://perma.cc/ZEC4-ZM3Q⟩ accessed 7 January 2021.

The Hague Centre for Strategic Studies, Launch of Global Commission on the Stability of Cyberspace (2017) ⟨https://perma.cc/VGQ3-XT8J⟩ accessed 26 November 2019.

The Hague Program for Cyber Norms, Dennis Broeders in Q&A and Discussion with Microsoft Global President and Chief Legal Counsel Brad Smith (2018) ⟨https://perma.cc/7C8J-78RV⟩ accessed 29 August 2020.

— 2019 Conference on Cyber Norms: Dealing with Uncertainty (2019) ⟨https://perma.cc/9XT4-YL92⟩ accessed 29 August 2020.

— Dennis Broeders at Working Dinner on Cyber Norms Paris Call, What Next? (2019) ⟨https://perma.cc/U63K-E3DX⟩ accessed 29 August 2020.

— Hague Program for Cyber Norms (2020) ⟨https://perma.cc/J2GE-7UMM⟩ accessed 29 August 2020.

— News and Events (2020) ⟨https://perma.cc/9F8S-NNV9⟩ accessed 29 August 2020.

— Research and Publications (2020) ⟨https://perma.cc/EM9N-6UDV⟩ accessed 29 August 2020.

Thomas R, *Blending Qualitative & Quantitative Research Methods in Theses and Dissertations* (SAGE Publications 2003) ⟨http://perma.cc/U6BV-FKNB⟩.

Thomas TL, *Information Security Thinking: A Comparison Of US. Russian, and Chinese Concepts* (techspace rep, Foreign Military Studies Office 2001) ⟨https://perma.cc/X642-856Y⟩.

Thompson DF, 'Moral Responsibility of Public Officials: The Problem of Many Hands' (1980) 74(4) American Political Science Review 905 ⟨https://perma.cc/S9ND-RRQD⟩.

Tikk E, Kaska K, and Vihul L, *International Cyber Incidents: Legal Considerations* (techspace rep, NATO Cooperative Cyber Defence Centre of Excellence 2010) ⟨https://perma.cc/7XMT-5YCA⟩.

Tikk E and Kerttunen M, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy' (2017) ⟨https://perma.cc/Q7PD-NEJG⟩.

Tikk E and others, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (Tikk E ed, United Nations Office for Disarmament Affairs 2017) ⟨https://perma.cc/N6KK-GKLT⟩.

Tikk-Ringas E, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee* (techspace rep, ICT4Peace Publishing 2012) ⟨https://perma.cc/VS34-DPXX⟩.

— 'International Cyber Norms Dialogue as an Exercise of Normative Power' (2016) 17(3) Georgetown Journal of International Affairs 47 ⟨https://perma.cc/J33H-KFA9⟩.

Toope SJ, 'Emerging Patterns of Governance and International Law' in M Byers (ed), *The Role of Law in International Politics* (Oxford University Press 2001) ⟨https://perma.cc/W6PZ-844D⟩.

Tor U, ''Cumulative Deterrence' as a New Paradigm for Cyber Deterrence' (2017) 40(1-2) Journal of Strategic Studies 92 ⟨https://perma.cc/Q8EF-T5GH⟩.

Trend Micro, ShadowPad Backdoor Found in Server Management Software (2017) ⟨https://perma.cc/2Q5X-LPU6⟩ accessed 31 March 2020.

Tsagourias N, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (2016) 21(3) Journal of Conflict and Security Law 455 ⟨https://perma.cc/924K-AAJ8⟩.

— 'The Slow Process of Normativizing Cyberspace' (2019) 113 AJIL Unbound 71 ⟨https://perma.cc/4TGK-WQJN⟩.

Tsuchiya M, A Difficult Road to International Norms for Cybersecurity (2019) ⟨https://perma.cc/6MF2-S3BJ⟩ accessed 8 December 2019.

Tuckett AG, 'Applying Thematic Analysis Theory to Practice: A Researcher's Experience' (2005) 19(1-2) Contemporary Nurse 75 ⟨https://perma.cc/BP3B-HHAC⟩.

Tullio T, 'Law of the Sea' in *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2011) ⟨https://perma.cc/WD4W-TR9A⟩.

USDepartment of Homeland Security, DHS Statement on the Issuance of Binding Operational Directive 17-01 (2017) ⟨https://perma.cc/462A-ML4E⟩ accessed 1 April 2020.

Ulbert C, 'How to Hit a Moving Target: Assessing the Effectiveness of Public-Private Partnerships' in H Hegemann, R Heller, and M Kahl (eds), *Studying 'Effectiveness' in International Relations: A Guide for Students and Scholars* (Verlag Barbara Budrich 2012).

Underdal A and Young OR, *Regime Consequences: Methodological Challenges and Research Strategies* (Springer Netherlands 2004) ⟨https://perma.cc/8VL6-NYHK⟩.

United Kingdom's Multi-Stakeholder Advisory Group on Cyber Issues, *Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015* (techspace rep, Chatham House 2019) ⟨https://perma.cc/357C-4C7G⟩.

United Nations Conference on Trade and Development, Data Privacy: New Global Survey Reveals Growing Internet Anxiety (2018) ⟨https://perma.cc/NGT3-RHNC⟩ accessed 26 February 2019.

United Nations Economic and Social Council, Progress Made in the Implementation of and Follow-Up to the World Summit on the Information Society Outcomes at the Regional and International Levels (2019) ⟨https://perma.cc/FPF9-LMYR⟩.

United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (1998) ⟨https://perma.cc/SV8C-6Q53⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (1999) ⟨https://perma.cc/BM5B-M93Z⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2000) ⟨https://perma.cc/4K4W-KV4N⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2001) ⟨https://perma.cc/9GLP-XKNN⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2002) ⟨https://perma.cc/4ZZJ-995B⟩.

— Responsibility of States for Internationally Wrongful Acts (2002) ⟨https://perma.cc/5TMJ-KA5A⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2003) ⟨https://perma.cc/SY9J-7VFC⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2005) ⟨https://perma.cc/XGY6-SSZY⟩.

— *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, 2010) ⟨https://perma.cc/LSD7-2YE7⟩.

— *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, 2013) ⟨https://perma.cc/X28E-M84A⟩.

— *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, A/70/174, 2015) ⟨https://perma.cc/KDE8-33PM⟩.

— Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (2018) ⟨https://perma.cc/3TU5-GJX9⟩.

— Developments in the Field of Information and Telecommunications in the Context of International Security (2018) ⟨https://perma.cc/5RGC-UCSK⟩.

United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (techspace rep, A/HRC/38/35, 2018) ⟨https://perma.cc/4PYE-S97W⟩.

United Nations Internet Governance Forum, Best Practice Forum on Cybersecurity (2019) ⟨https://perma.cc/W5M4-NNP3⟩ accessed 7 December 2019.

— *Cybersecurity Agreements: Final BPF Output Report* (techspace rep, United Nations Internet Governance Forum 2019) ⟨https://perma.cc/VN5D-76P8⟩.

— IGF 2019 BPF on Cybersecurity Contributes to UN OEWG (2019) ⟨https://perma.cc/9DGA-L7QY⟩ accessed 28 August 2020.

— Best Practice Forums (2020) ⟨https://perma.cc/4VDQ-4SPL⟩ accessed 28 August 2020.

United Nations Office on Drugs and Crime, *Group of 77 Workshop on Preventing and Combating Cybercrime supported by the Russian Federation and the United Nations Office on Drugs and Crime* (techspace rep, United Nations Office on Drugs and Crime 2018) ⟨https://perma.cc/JUF5-BFG5⟩.

United Nations Open-ended Working Group, *Second Pre-Draft of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security* (techspace rep, United Nations 2020) ⟨https://perma.cc/6ADQ-TF2D⟩.

Untersinger PM, La France Veut Relancer les Négociations Sur la Paix Dans le Cyberespace (2018) ⟨https://perma.cc/FUH3-HYMV⟩ accessed 19 August 2019.

US Department of Defense, *DoD Dictionary of Military and Associated Terms* (techspace rep, 2019) ⟨https://perma.cc/P9NS-NJWW⟩.

Valeriano B and Maness RC, 'Cyber Conflict and Non-State Actors' in *Cyber War Versus Cyber Realities* (Oxford University Press 2015) ⟨https://perma.cc/K573-E6AQ⟩.

Van Horenbeeck M, FIRST Address to the Global Commission on the Stability of Cyberspace (2018) ⟨https://perma.cc/B8SD-GUUY⟩ accessed 27 November 2018.

— The Operationalization of Norms and Principles on Cybersecurity (2019) ⟨https://perma.cc/42ZF-DR7J⟩ accessed 7 December 2019.

Vihul L, The Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) ⟨https://perma.cc/P4FM-HQHP⟩ accessed 23 February 2018.

Volz D and Schectman J, McAfee Says It No longer Will Permit Government Source Code Reviews (2017) ⟨https://perma.cc/2ZDC-YLRZ⟩ accessed 18 August 2019.

Wach E, Ward R, and Jacimovic R, *Learning about Qualitative Document Analysis* (techspace rep, August, Institute of Development Studies 2013) ⟨https://perma.cc/Y9M5-W6FQ⟩.

Wagner M, 'Non-State Actors' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2009) ⟨https://perma.cc/H4JV-SWDB⟩.

Waxman MC, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36(2) Yale Journal of International Law 421 ⟨https://perma.cc/BF5K-D83Y⟩.

Weber RH, 'Accountabililty in Internet Governance' (2009) 13 International Journal of Communications Law and Policy 152 ⟨https://perma.cc/SW88-9FAG⟩.

Webley L, 'Qualitative Approaches to Empirical Legal Research' in P Cane and HM Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010) ⟨https://perma.cc/J5AJ-D5H2⟩.

Weissbrodt D, 'Roles and Responsibilities of Non-State Actors' in D Shelton (ed), *The Oxford Handbook of International Human Rights Law* (Oxford University Press 2013) ⟨https://perma.cc/YYU7-PLVQ⟩.

Wendt A, 'The Agent-Structure Problem in International Relations Theory' (1987) 41(3) International Organization 335 ⟨https://perma.cc/H88V-XHMZ⟩.

— 'Anarchy Is What States Make of It' (1992) 46(2) International Organization 391 ⟨https://perma.cc/V3WX-UCJR⟩.

— 'Constructing International Politics' (1995) 20(1) International Security 71 ⟨https://perma.cc/C8HE-SS93⟩.

— *Social Theory of International Politics* (Cambridge University Press 1999).

Wex Legal Dictionary, Opinio Juris (2018) ⟨https://perma.cc/WTV6-YNJD⟩ accessed 23 October 2018.

Wheatley S, 'Democratic governance beyond the state: the legitimacy of non-state actors as standard setters' in A Peters and others (eds), *Non-State Actors as Standard Setters* (Cambridge University Press 2009) ⟨https://www.cambridge.org/core/product/identifier/CBO9780511635519A023/type/book_part⟩.

Whitman ME and Mattord HJ, *Management of Information Security* (Cengage Learning 2017).

Whitman ME and others, *Guide to Network Security* (Cengage Learning 2012).

Wiener A, 'The Dual Quality of Norms and Governance Beyond the State: Sociological and Normative Approaches to Interaction' (2007) 10(1) Critical Review of International Social and Political Philosophy 47 ⟨https://perma.cc/DUD5-WRCR⟩.

— *The Invisible Constitution of Politics: Contested Norms and International Encounters* (Cambridge University Press 2008).

— *A Theory of Contestation* (Springer 2014).

Williams O, Exclusive: Kaspersky's Global Transparency Initiative Fails to Convince UK Government (2018) ⟨https://perma.cc/JW5K-ML22⟩ accessed 29 August 2020.

Willis B, 'The Advantages and Limitations of Single Case Study Analysis' [2014] E-International Relations 1 ⟨https://perma.cc/KMJ5-MU7V⟩.

Willis J, *Foundations of Qualitative Research: Interpretive and Critical Approaches* (SAGE Publications 2007) ⟨http://perma.cc/95EZ-8N6K⟩.

Winston C, 'Norm Structure, Diffusion, and Evolution: A Conceptual Approach' (2018) 24(3) European Journal of International Relations 638 ⟨http://perma.cc/76X3-A348⟩.

Wolf KD, 'Output, Outcome, Impact: Focusing the Analytical Lens for Evaluating the Success of Corporate Contributions to Peace-Building and Conflict Prevention' (2010) ⟨https://perma.cc/STL2-35UH⟩.

Wolfers A, 'National Security as an Ambiguous Symbol' (1952) 67(4) Political Science Quarterly 481 ⟨https://perma.cc/E7A3-BQ28⟩.

Wolff J, 'What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates' (2016) 5(3) Internet Policy Review 1 ⟨https://perma.cc/6TC6-W33F⟩.

World Bank, Civil Society (2020) ⟨https://perma.cc/ZU4Q-97YJ⟩ accessed 29 August 2020.

World Economic Forum, *The Future Role of Civil Society* (techspace rep, January, World Economic Forum 2013) ⟨https://perma.cc/8DJX-SNDV⟩.

— *The Global Risks Report 2020* (techspace rep, World Economic Forum 2020) ⟨https://perma.cc/TJ9K-TXSJ⟩.

World Health Organisation, *WHO Accountability Framework* (techspace rep, March, World Health Organisation 2015) ⟨https://perma.cc/7FV4-Y3T8⟩.

World Wide Web Consortium, World Wide Web (2019) ⟨https://perma.cc/9FAZ-SCGL⟩ accessed 31 March 2019.

Wright J, Cyber and International Law in the 21st Century (2018) ⟨https://perma.cc/JT3C-JZP8⟩ accessed 28 May 2018.

Wu TS, 'Cyberspace Sovereignty? The Internet and the International System' (1998) 10(3) Harvard Journal of Law & Technology 647 ⟨https://perma.cc/4LEU-KQB4⟩.

Yang Y, The Great Firewall of China: Web of Control (2019) ⟨https://perma.cc/A4VY-AS8F⟩ accessed 13 April 2019.

Yilmaz K, 'Comparison of Quantitative and Qualitative Research Traditions: Epistemological, Theoretical, and Methodological Differences' (2013) 48(2) European Journal of Education 311 ⟨https://perma.cc/EAB3-A7EA⟩.

Zetter K, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishers 2014).

Zimmermann L, Deitelhoff N, and Lesch M, 'Unlocking the Agency of the Governed: Contestation and Norm Dynamics' (2017) 2(5) Third World Thematics: A TWQ Journal 691 ⟨https://perma.cc/379P-5DYA⟩.

Zürn M, 'Global Governance as Multi-Level Governance' in D Levi-Faur (ed), *The Oxford Handbook of Governance* (Oxford University Press 2012) ⟨https://perma.cc/QK5N-8MD7⟩.