Cyber Security Assemblages: The Theory and Practice of Diffuse Security Provision



Jamie Collier

St Cross College

University of Oxford

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

Michaelmas Term

2019

(83,779 words)

Abstract

Cyber security is typically provided by a highly complex and diffuse network of actors. Public, private, global, and local security providers operate within the same structures. The relationships between these actors are highly varied – cooperation, coordination and even conflict exist within these cyber security assemblages. Furthermore, the distinctions between actors are often blurred as hybrid structures emerge.

This thesis explores the implications of these trends on cyber security outputs and international relations. Three case studies examine the cyber security of critical national infrastructure in the UK, encryption in the US, and digital society in Estonia. The type of actors providing cyber security (including their incentive structures and resources), the relationships between actors, power dynamics, and levels of fusion are all found to have an influential bearing on the nature of cyber security provision.

In developing these ideas, it is argued that examining security actors is an important, yet often neglected component of cyber insecurity. While much attention is paid towards threat actors and the structure of cyber conflict, an examination of who provides cyber security and the dynamics discussed above remains comparatively underexplored. This thesis therefore seeks to develop theoretical, conceptual and empirical findings that emphasise the importance of thinking about security provision.

Table of Contents

ABSTRACT 3

TABLE OF CONTENTS 5

CHAPTER ONE: DIFFUSE CYBER SECURITY STRUCTURES 8

Introduction and Research Question 8

Thinking with Security Assemblages 20

Cyber Security Assemblages 31

Methods 44

Chapter Summaries 55

CHAPTER TWO: CYBER SECURITY ASSEMBLAGE THEORY BUILDING 59

Theoretical Model 59

Assemblage Configuration 61

Assemblage Dynamics 71

Security Outputs 78

Applying the Theoretical Model to the Case Studies 82

CHAPTER THREE: THE US ENCRYPTION SECURITY ASSEMBLAGE 84

Introduction 84

Encryption in the United States: A Contextual History 85

Assemblage Configuration: dispersed power and fragmented incentives 89

Corporations 90
Government actors 98
International Organisations and Networks 110
Knowledge, Advocacy, and Pressure Groups 112
Media and News Outlets 114
Academic Actors 116

Assemblage Dynamics: unstable and contentious disputes 118

Internal Workings of the US Encryption Security Assemblage 118
The Assemblage Configuration has a clear bearing on the internal dynamics within the US Encryption Assemblage. The number of actors, alongside the variety of incentive structures and the diffusion of power across various actors are crucial variables that have led to both disharmony and fragmentation. There is a significant lack of fusion with the majority of actors ontologically distinct and possessing their own agency and set of motivations. The practices within the US Encryption Assemblage drive wedges between actors. Tensions exist on three accounts within the assemblage: conflict between strong and weak-encryption

clusters, conflict within each of these inter-unit clusters and tensions within traditional units (most notable when examining the dynamics between US Government actors). 118
Evolution: technical, political and legal instability 127
Example One: The Snowden Fallout 132
Example Two: Apple vs FBI 135

Security Outputs: iterative security 138

US Encryption Security Assemblage Conclusion 143

CHAPTER FOUR: THE UK CRITICAL NATIONAL INFRASTRUCTURE SECURITY ASSEMBLAGE 146

Introduction 146

A Background of UK Critical National Infrastructure 148

Assemblage Configuration: corporation-led security and public-private fusion 153
Government Actors 153
Corporations 160
International Actors and Networks 168
Academic Actors 174

Assemblage Dynamics: the competition of security provision and entrenched partnership structures 177
Internal Workings of the UK CNI Assemblage 177
Evolution: from market forces to market failure 189
Example One: Foreign involvement in the UK CNI Assemblage 193
Example Two: shifts in official UK Government cyber security strategy on the role of the market 197

Security Outputs: market failure 199

UK CNI Security Assemblage Chapter Conclusion 208

CHAPTER FIVE: THE ESTONIAN DIGITAL SOCIETY SECURITY ASSEMBLAGE 210

Introduction 210

Estonia's Digital Society: Overcoming the Legacy of the Soviet Union 211

Assemblage Configuration: a decisive government amidst volunteer and international actors 217
Government Actors 217
Civilian Groups 223
Corporations 225
International Organisations, Networks, and Partners 228

Assemblage Dynamics: hybrid and harmonious relationships within a small state 233
Internal Processes 233
Evolution 242
Example One: Cyber security volunteerism 245
Example Two: Estonia's Data Embassy project 247

Security Outputs: individual security at the core 249

Estonia Digital Society Assemblage Chapter Conclusion 253

CHAPTER SIX: CONCLUSION AND THE CASE FOR STUDYING CYBER SECURITY PROVISION 256

Thesis Findings and Core Arguments **256**

Implications for Theory and Practice **267**

Future Research and Conceptual Avenues **275**

BIBLIOGRAPHY 280

Primary Sources **280**
Interviews 280
Official Government and International Organisation Bills, Documents, Hearings, Reports, and Committee Evidence 281
Statements and Speeches 286
Legal Acts and Documents 287
Public Opinion Polls 288

Secondary Sources **288**
Academic Publications 288
Industry and think-tank reports and documents 297
Patents 299
Film and Videos 299
News and websites 299

Chapter One: Diffuse Cyber Security Structures

Introduction and Research Question

Cyber security is provided by a vastly complex configuration of actors. A range of non-state and other non-traditional actors are at the forefront of contemporary cyber security challenges: private sector firms,[1] hacktivist groups,[2] intergovernmental organisations,[3] and volunteer networks[4] all provide (or threaten) security in some important way. Whether it be the historically prominent role of private actors in the development and growth of cyber-related industries, or the low barriers to entry, non-traditional actors have developed meaningful capabilities.[5] Cyber security is therefore typically provided by a diffuse network of security providers, rather than a single uniform actor such as a state in the traditional Weberian sense.[6]

The complex configuration of cyber security actors is interesting, not just because of its idiosyncrasies, but also because of its disruptive effects on mechanisms of statecraft. States cannot take their standing as the primary security provider for granted (as is now the case in

[1] Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," *Cyber Studies Working Paper Series* 1 (2015); Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (January 2016): 43–62.
[2] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London, UK: Verso, 2014); Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency* (London, UK: William Heinemann, 2013).
[3] "NATO Cyber Defence Fact Sheet" (NATO, July 2016), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf; "EU Cybersecurity Initiatives Working Towards a More Secure Online Environment" (European Commission, January 2017), http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.
[4] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?," *Studies in Conflict & Terrorism* 36, no. 9 (September 2013): 777–87; Rain Ottis, "From Pitchforks to Laptops Volunteers in Cyber Conflicts" (Conference on Cyber Conflict, Tallinn, Estonia: NATO CCDCOE, 2010), 97–109, https://ccdcoe.org/publications/2010proceedings/Ottis%20-%20From%20Pitchforks%20to%20Laptops%20Volunteers%20in%20Cyber%20Conflicts.pdf.
[5] Joseph S Nye Jr, *The Future of Power*, (New York: Public Affairs, 2011). pp. 113-152.
[6] This relates to Max Weber's claim that state hold a 'monopoly of the legitimate use of physical force within a given territory.' See, Max Weber, "Politics as a Vocation," in *From Max Weber: Essays in Sociology*, ed. Hans Heinrich Gerth and Charles Wright Mills (Abingdon, UK: Routledge, 2009), 77–128.

numerous security contexts).[7] Various security actors work together to provide cyber security with a shared understanding of hierarchy still being negotiated and defined (and often a source of considerable tension). Government actors may therefore find not only their capabilities, but also their legitimacy as a security actor fundamentally questioned. The flight of power away from state structures has produced what Lucas Kello called a 'sovereignty gap'[8] – private sector firms and individuals can no longer take their government's ability to protect them for granted (as they might in other security contexts). In certain instances, states have lost or relinquished both their authority and responsibility over cyber security.[9] In other contexts, however, states are actively challenging established private-sector norms and practices. The ambiguous and often shifting roles of security providers (both public and private) therefore represent a consistent and disruptive theme in the organisation of cyber security provision.

As significant as the diffuse nature of security provision might be, it remains under-analysed and regularly misunderstood within a cyber security context. The majority of cyber security literature within IR and the sub-discipline of security studies has either focused on the supposed inherent difficulties of delivering cyber security (whether due to claimed difficulties in attribution, the apparent offence-dominant context, etc.) or on cyber threat actors and their activity. Focus on security providers, and the implications that derive from diffuse security structures remains comparatively under-explored.[10] Yet, it is here that IR theory offers so much

[7] Peter W Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, (Ithaca, NY: Cornell University Press, 2008); Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (New York: Oxford University Press, 2014); Andrew Mumford, *Proxy Warfare* (Cambridge, UK: Polity Press, 2013); Andrew Mumford, "Proxy Warfare and the Future of Conflict," *The RUSI Journal* 158, no. 2 (April 2013): 40–46.
[8] Lucas Kello, *The Virtual Weapon and International Order*, (New Haven, CT: Yale University Press, 2017) 160-162.
[9] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies."
[10] Notwithstanding the excellent contributions already made. For instance, see Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (December 2009): 1155–75; Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better" (2012 4th International Conference on Cyber Conflict, Tallinn, Estonia, 2012), 141–53; Ronald J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium* 32, no. 3 (December 2003): 501–30; Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, Canada: Signal, 2013).

in providing at a better understanding and framing of these issues. Whether it be actor-network theory, the Copenhagen School, the emergence of disaggregated sovereignty, or the notion of a military–industrial complex, IR literature brings a wealth of theories and conceptual tools that help to make sense of the issues related to diffuse security structures and contested security. Despite the historical focus on nation states in IR literature, these issues are by no means foreign to the discipline. Critical security studies literature also brings much to studying cyber security provision through theories and concepts that elucidate the perils and consequences that can arise from security practices – trends such as securitisation, militarisation and leaving vulnerable stakeholders unrepresented are all issues highly relevant to cyber security. Various studies have made important advances by exploring how these ideas apply to cyber security in order to understand the often flawed nature of security provision.[11] The diffusion of security has also been examined through research that has focused on specific forms of relationships between security actors including public-private partnerships,[12] multi-stakeholder approaches,[13] and states' use of proxy actors.[14] Many of these developments are important and certainly deserve analysis in their own right, yet current literature on diffuse cyber security

[11] ibid.
[12] Carr, "Public–Private Partnerships in National Cyber-Security Strategies."; Myriam Dunn-Cavelty and Manuel Suter, "Public–Private Partnerships Are No Silver Bullet: an Expanded Governance Model for Critical Infrastructure Protection" 2, no. 4 (December 1, 2009): 179–87; Myriam Dunn Cavelty, "Cyber-Security and Private Actors," in *Routledge Handbook of Private Security Studies*, ed. Rita Abrahamsen and Anna Leande, (Abingdon, UK: Routledge, 2015), 65–71; Peter W Singer and Allan Friedman, *Cybersecurity and Cyberwar*, (New York : Oxford University Press, 2014).
[13] Lilly Muller, "How to Govern Cyber Security? The Limits of the Multi-Stakeholder Approach and the Need to Rethink Public-Private Cooperation," in *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, ed Karsten Friis and Jens Ringsmose (Abingdon, UK: Routledge, 2016), 116–29; Madeline Carr, "Power Plays in Global Internet Governance," *Millennium: Journal of International Studies* 43, no. 2 (January 2015): 640–59.
[14] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers, (Tallinn, Estonia: NATO CCDCOE, 2015), 79–86; Gregory J Rattray and Jason Healey, "Non-State Actors and Cyber Conflict," in *Americas Cyber Future Security and Prosperity in the Information Age*, ed. Kristin M Lord and Travis Sharp (Washington, DC: Center for a New American Security, 2011), 65–86; Michael N Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: the Evolving International Law of Attribution," *Fletcher Security Review* 1, no. 2 (June 26, 2014): 53–72.

structures lacks broader frameworks that are able to capture the shifting security governance landscape through a cohesive and systemic lens.

The complexity of security provision in the cyber domain means that it is difficult to capture ongoing shifts in power with uniform theories and simple narratives. In truth, various simultaneous and yet seemingly contradictory trends coexist, albeit unhappily. For example, states are simultaneously undermining and being undermined by private actors. Private actors may compete against states while working directly with them in separate contexts. Tired references to the weaknesses of state actors in the cyber domain often neglect to mention the substantial increase in investment occurring within many government cyber security programmes[15] or the fact that the vast majority of sophisticated cyber operations stem from government agencies.[16] While the process of power diffusion and the emergence of non-state actors is significant, there is also a risk of making too strong a claim of cyber exceptionalism,[17] ignoring the diffuse nature of security structures that exist in non-cyber contexts. At the same time, direct comparison with other security contexts would often be misplaced. Taking the role of outsourcing in traditional military contexts[18] as an example, while the issue has parallels to cyber security (on the basis that multiple non-state actors are involved in security), the formation of security structures in these two contexts are nonetheless altogether different.

[15] For example, the US 2019 federal budget for cyber security-related activities is $15 billion while the UK has doubled its cyber security spending to £1.9 billion for the 2016-2021 period. See, "Cybersecurity Funding" (The White House, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf; "Britain's Cyber Security Bolstered by World-Class Strategy," GOV UK, November 1, 2016, https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.

[16] The US-Israeli cyber operation that targeted Iranian nuclear facilities in 2010 known as Stuxnet provides the best example of this. A more recent example of a destructive state cyber operation would be the NotPetya ransomware deployed by Russia in 2017. See, Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32 Stuxnet Dossier" (Symantec, February 2011), https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014); Iain Thomson, "Everything You Need to Know About the Petya, Er, NotPetya Nasty Trashing PCs Worldwide," The Register, June 28, 2017, https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

[17] Max Smeets and James Shires, "Cyber Exceptionalism," New America, December 7, 2017, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/cyber-exceptionalism/.

[18] Peter W Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*.

While in traditional military functions, what were government functions have been outsourced to contractors,[19] in cyber security, by contrast, states have often expanded their security role and acquired new functions – often, in fact, challenging or taking over from private firms during this process.[20]

Before evaluating these realities, it is first necessary to outline the terms used in this thesis. Cyberspace is defined as an environment formed by physical and non-physical components and characterised by the use of computers and other networked devices. Cyber security, by extension, refers to the security of cyberspace. That is, the confidentiality, integrity and availability of data, as well as the underlying infrastructure (including network infrastructure, routers, cables, etc.). The cyber domain refers to a broader social space or realm of interaction associated with cyberspace. Of course, almost all anyone or anything could now be said to be associated with computers and the internet – for the purposes of this thesis, the term is narrowed to comprise the key actors involved more directly (such as prominent technology firms, signals intelligence agencies, hacker groups, etc.).

This thesis seeks to make sense of how public and private, and global and local, actors work together (or against each other) and become increasingly embedded in the provision of cyber security. Here, it is not conducive to blindly impose traditional IR theories and concepts to the issue of cyber security in a rigid, top-down manner. Applying traditional approaches also involves importing certain logics that risk oversimplifying the messy realities of the cyber domain in order to fit within pre-existing paradigms. Rather than helping to elucidate our

[19] Peter W Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*; Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order*; Andrew Mumford, *Proxy Warfare*; Andrew Mumford, "Proxy Warfare and the Future of Conflict."

[20] Examples would include the FBI challenging Apple's encryption stance and the recently introduced Global Data Protection Regulation. See, Mark Weinstein, "FBI vs Apple: Defining Our Constitutional Future," Huffington Post, February 19, 2016, https://www.huffingtonpost.com/mark-weinstein/fbi-vs-apple-defining-our_b_9260606.html; "Security," Information Commissioner's Office, May 18, 2018, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/.

understanding of cyber security, traditional theories risk blunting them instead. Taking a different approach, this thesis begins with a more inductive, bottom-up analysis – that considers which actors provide cyber security and how the configuration of various actors affects cyber security – with the following central research question:

How does the configuration of security actors, and the dynamics between these actors, influence the provision of cyber security?

This thesis seeks to better understand how the characteristics of security providers, and how the interactions between security, influence security provision. Whilst it is axiomatic that a link exists between the makeup of security providers and eventual security outcomes, this process is not sufficiently understood. The majority of cyber security contexts contain a highly complex configuration of security actors, yet empirical research has not sufficiently explored the implications of these often crowded security structures. Although it is clear that the configuration of security actors matter, it remains unclear *how* they matter. As primarily an exploratory project, this thesis will seek to unearth and identify important variables related to security providers that have an influential bearing on security provision. It is this endeavour that forms the primary aim (and contribution) of this thesis.

It is argued that within the majority of cyber security contexts, a complex configuration of security actors exists. This thesis will make the case that these structures deserve greater attention. The distribution of power within a network of security actors; the disagreements and areas of contestation that exist; the extent (or lack of) cooperation; the way in which actors can merge together or become entrenched – all of these issues have fundamental implications for how cyber security is provided. The findings of this thesis show that by examining security actors and their characteristics (i.e. their incentive structures, capabilities, and the institutional

context they sit within) are all crucial variables in understanding contemporary cyber security challenges.

Hybridity takes on a central theme throughout the thesis, defined as the amalgamation that exists between entities in an assemblage. The concept considers the extent to which ontological distinctions between actors remains coherent and justified. Traditionally-held distinctions (such as those between public and private, or global and local) serve an important function in organising the world into decisive categories. However, their coherence is being challenged. A review of existing literature below will show that this is not a new issue, nor one that applies exclusively to cyber. Yet, if traditional distinctions are being questioned, cyber security structures exemplify why. Diffuse cyber security structures do not just comprise a variety of organisations and institutions, but also show how what have often been considered ontologically distinct actors are merging together. The extent of hybridity (a term used interchangeable with fusion) exists on a spectrum – while in certain contexts the distinctions between different actors and organisations are blurring, in other areas they remain clearly distinct. In addition to acknowledging these hybrid structures, this thesis seeks to go further by understanding their dynamics and the implications that they have for security provision.

Important research has already explored many of these topics. This thesis seeks to build on this work by developing a conceptual framework that brings a variety of the themes related to the challenges and tensions of diffuse security provision into a cohesive narrative. In doing so, there is an ambition to add to literature that emphasises the importance of thinking about cyber security providers themselves – as opposed to research that emphasises the structural causes of cyber insecurity or that focuses on the threat landscape.

Empirically, the thesis develops this argument in three case studies – critical national infrastructure (CNI) in the UK, encryption in the US, and digital society in Estonia. The

primary aim is to understand what the provision of cyber security looks like and what the configuration of, or relationships between, public and private, and global and local, security actors mean for the provision of cyber security. Here, in addition to providing a rich account of highly relevant issues for IR and security studies, these three case studies also serve to narrow the scope of the research project. The central enquiry of this thesis is interpretive in nature. There is an ambition to provide a broader understanding of cyber security provision by proposing a framework and theoretical approach that can fully accommodate the complexity of cyber security provision at hand. This approach should offer a more nuanced and detailed account of cyber security provision – an alternative to the traditional theories that risk oversimplification. Through an interpretative approach, it is possible to establish the configuration and dynamics of assemblages, and explore how these variables affect cyber security provision. Emphasis is therefore placed on *understanding* as opposed to *explaining*.[21]

An explanatory approach to the analysis of cyber security agency that seeks to establish causal mechanisms is avoided, yet such an approach should not be wholly dismissed. While the IR discipline has been subsumed by a variety of debates over the nature of research,[22] epistemological tribalism ultimately curtails the value that can be derived from different scientific approaches coexisting.[23] Positivist projects examining cyber security providers and diffuse security network would no doubt represent a useful academic endeavour. Even within the central research question outlined above, there lies an implicit assumption that the complex configuration of security actors has implications for the provision of cyber security. An in-depth causal analysis could explore this further, perhaps testing the causal mechanisms that

[21] Martin Hollis and Steve Smith, *Explaining and Understanding in International Relations*, (Oxford, UK: Oxford University Press, 1991).
[22] Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994); James Mahoney, "After KKV: The New Methodology of Qualitative Research," *World Politics* 62, no. 1 (2010): 120–47.
[23] Patrick Thaddeus Jackson, *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics* (Abingdon, UK: Routledge, 2011).

affect the configuration of security actors in a particular context or how the different types of relationships between, say public and private actors, affect mechanisms of security provision. Such a project would undoubtedly aid policymakers and security actors in developing successful security models.

Yet, an explanatory approach would currently be premature, despite its potential benefits. Cyber security studies remains in its early stages from an international relations and security studies perspective. There is therefore a need to propose, build up, and develop appropriate conceptual frameworks in which to explore relevant issues. The applicability of the concepts and theories traditionally used in IR should first be questioned when determining their application to a nascent security context.[24] As Kello argues, 'conceptual frameworks can be altered by the very technology that scholars seek to interpret, possibly leading to theoretical breakthroughs. Accordingly, past generations of thinkers have tended to respond to technological revolutions by at least testing their concepts against them.'[25] A positivist approach that takes such traditional terms and frameworks as its starting point therefore risk oversimplifying the realities of the cyber domain.

It is also not at currently clear what variables might be relevant or not in testing issues related to the provision of cyber security. Methodological hurdles related to data availability could also inhibit such an approach. Although data-related challenges also apply to interpretive projects (as discussed in the methods section of this chapter), the issue is more profound when seeking to confidently establish (or rule out) relevant causal variables – given the extent of the claim being made. Here, it is hoped that this thesis will contribute to making sense of security

[24] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."
[25] ibid.

provision in the cyber domain as a broader interpretive project and thereby make inroads towards establishing a foundation that makes other forms of enquiry more viable in the future.

The theory-building ambitions of this thesis seek to address and rectify some of the current problems associated with theory-testing projects. For the purposes of this thesis, IR theory is defined as conceptual frameworks or lenses used to articulate and view international affairs. Rather than just capturing trends and processes related to contemporary cyber security provision, there is an ambition, if not to test, but to identify and propose two sets of possible causal variables that would merit further analysis going forward. The first, explores how the configuration of a security structure (i.e. the relevant security actors involved, their incentive structures, and their resources or capabilities) affects the internal dynamics within a security structure (i.e. the extent to which hybrid structures have emerged, the harmony and relationships between security actors, and the evolutionary processes that occur). If it is not the state that provides cyber security, then it is necessary to understand which actors provide security. Outlining the relevant security actors brings attention to the sheer variety of actors involved in the provision of cyber security. With a range of actors providing cyber security, a variety of incentive structures naturally exist.[26] When interests between actors overlap, cooperation amongst stakeholders is certainly feasible. Conversely, diverging interests can represent a clear source of tension that can lead to competition and even rivalry between security actors. Likewise, turning to power, even if government actors operate in a crowded space amongst other non-state cyber security actors, this is not intrinsically significant unless these other non-state actors possess meaningful power and capabilities. Thinking about the different security actors, as well as their motivations and power, are therefore crucial when understanding the dynamics of a diffuse security structure.

[26] Madeline Carr, *US Power and the Internet in International Relations* (London, UK: Palrave Macmillan, 2016).

The second set of variables will consider how both the configuration and internal dynamics of a security structure then affect material security outputs – or in other words, how these issues affect the notion of security that states and citizens receive. It is important to understand how different motivations and visions of security come together: whether they are compatible or mutually exclusive, how clashing securities create disruption and establishing the dominant notion of security that endures.

State-centric paradigms can provide a coherent theoretical lens to explore cyber security provision and the emergence of more diffuse and non-state networks can often yields useful insights.

One school of thought has presented the emergence of private actors in opposition to state authority and the public provision of security. As the private security sector has expanded and globalised, debate has followed on the extent to which the state is losing power and sovereignty, thereby becoming weaker as private actors strengthen their capability.[27] This narrative can and has been applied to cyber security contexts. Whilst Nye acknowledges that states remain the most powerful actors in the cyber domain in absolute terms, he has argued that states are relatively less powerful in the cyber domain, caused by a power diffusion process that has empowered non-state actors due to the low costs and barriers to entry, as well as their inherent flexibility and adaptability.[28] It has also been highlighted that developments in the cyber domain often outpace regulatory timelines, thereby leading to lethargic policy responses by governments.[29]

[27] Michael C Williams, "Global Security Assemblages," in *Routledge Handbook of Private Security Studies*, ed. Rita Abrahamsen and Anna Leande, 2016.
[28] Joseph S Nye Jr, *The Future of Power*, 113-152.
[29] For example, US Congress failed to pass a single piece of major cyber security legislation between 2002 and 2014 and it took the US Federal Risk and Authorisation Management Program six months to approve its first contractor. Although six months was regarded as fast within government, given the relevant bureaucratic hurdles to be negotiated, the pace was regarded as sluggish amongst the wider cyber security community. See Peter W Singer and Allan Friedman, *Cybersecurity and Cyberwar*.

Others have made the contrasting argument: the rise of private security actors has been analysed as part of new forms of multi-level governance that enhance the standing of states. Here, the state has outsourced its security functions and continues to rule and regulate from a distance in collaboration with a range of non-state actors.[30] Others have gone further in emphasising the role of state power throughout this process. During the 1970s and in the context of growing multinational corporations, Gilpin argued that when multinational corporations have influenced the international system, it has been via their home governments.[31] Multinational corporations therefore act as an extension of state power rather than a threat to it. Likewise, Krasner has argued that states often shape the conditions of the international system that allows multinational corporations to flourish. For example, the openness of the world economy, which largely facilitates the movement and growth of transnational multinational corporations, has correlated with periods where a state has enjoyed a high level of dominance in the international system (such as the UK in the nineteenth century and the US after World War II).[32]

These arguments also hold parallels in a cyber security context: the role of the US government in the emergence of the internet — and the subsequent emergence of dominant US private sector firms in the sector — should not be underestimated.[33] Likewise, technology that was designed initially for the US military has subsequently been passed on to US technology firms and played a decisive role in their growth within the international economy.[34] Neorealists might

[30] Sean McFate, *The Modern Mercenary*.
[31] Robert Gilpin, "The Politics of Transnational Economic Relations," in *Transnational Relations and World Politics*, ed. Robert O Keohane and Joseph S Nye Jr, 1973, 48–69.
[32] Stephen D Krasner, "State Power and the Structure of International Trade," *World Politics* 28 (1976): 317–46.
[33] Although much of the innovation came from the private sector, the US government still played an important role in its development. For example, a portion of the US Defense Advanced Research Projects Agency was designated to 'blue-sky thinking' that helped to fund the formation of computer science departments and provided start-up firms with early research support that partly facilitated the early stages of the internet. See Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, (London, UK: Anthem Press, 2014). pp. 76.
[34] For example, US military technology proved influential in the advent of the iPod and iPhone. See ibid.

also argue out that much of the global internet represents the values of the most powerful states such as the US and China (depending on the area or region studied).

These previous IR theories and arguments provide useful framing for understanding cyber security actors and security providers. While they may appear to contradict each other, all of these viewpoints are useful in some capacity; ultimately, opposing narratives often co-exist (albeit unhappily).

Nevertheless, despite the application of the theories and concepts outlined above, the central research question of this thesis is better served through theoretical approaches that emphasise both the decentralised and often hybrid nature of many contemporary security structures. The following section therefore outlines the core theoretical term used in this thesis: security assemblages.

Thinking with Security Assemblages

The concept of *security assemblages* is used as a means for understanding and articulating the configuration of actors within the cyber domain. The use of the term is part of an emerging body of scholarship within IR literature that seeks to empirically assess complex structures where a range of different global and local, and public and private security agents interact, cooperate and compete to produce new institutions, practices and forms of security governance.[35] An assemblage approach examines how state power and the provision of security might have been reconfigured as they increasingly sit in more diffuse structures. While assemblage thinking can examine state power, the more central idea is to consider how security

[35] Rita Abrahamsen and Michael C Williams, "Security Beyond the State: Global Security Assemblages in International Politics," *International Political Sociology* 3, no. 1 (March 1, 2009): 1–17; Abrahamsen and Williams, *Security Beyond the State;* Michele Acuto and Simon Curtis, eds., *Reassembling International Theory*, (Palgrave Macmillan, 2013).

institutions and practices that cross traditional boundaries are forming.[36] In the cyber domain this process has clearly been facilitated in cyber security contexts through a combination of the low barriers to entry that have enabled a variety of non-traditional actors to develop meaningful capabilities[37] as well as the inherent globalising qualities of the internet that have brought such actors together alongside more established players such as states. Pursuing assemblage thinking means paying attention to the relationships between a variety of actors and the forces that impel them to act in the way they do.[38] It moves away from the traditional locus of the nation-state to multi-layered, networked configurations that can accommodate a range of entities including (inter)governmental, para-governmental, nongovernmental, and private organisations.[39]

The concept's most defining characteristic is therefore its accommodation of the forces of globalisation and a scepticism of rigid state borders and distinctions. Such an approach instead seeks to capture a broader and often looser network of actors that is typically transnational and comprises both public and private actors. For example, in the context of the privatisation of security, Rita Abrahamsen and Michael Williams have argued that the process 'cannot be captured through the lens of public-private opposition but requires instead consideration of how these distinctions are being reconfigured into networks and practices indicative of new relations of power.'[40] Assemblage thinking therefore seeks to break with inside-outside distinctions and move towards a more holistic world view.

The point here is not to demonstrate that states are weaker in the cyber domain. Instead, the objective is to show that there is, in fact, a more complex configuration of actors that maintain

[36] This process is largely due to the dynamic nature of the international system where static concepts eventually expire.
[37] Joseph S Nye Jr, *The Future of Power*, 113-152; David Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower* (Abingdon, UK: Routledge, 2011).
[38] Debbie Lisle, "Energising the International," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis, (London, UK: Palgrave Macmillan, 2013), 67-74. pp. 72.
[39] Nadine Voelkner, "Tracing Human Security Assemblages," in *Research Methods in Critical Security Studies*, ed. Mark B Salter and Can E Mutlu, (Abingdon, UK: Routledge, 2013), 203-206. pp. 203.
[40] Rita Abrahamsen and Michael C Williams, *Security Beyond the State*, 12.

contingent and multifaceted relationships with each other – relationships that may not be captured by static and often state-centric theories. Contemporary security in fields such as the cyber domain are replete with global and local, public and private agents whose relationships are deeply competitive as well as cooperative, conflictual, and at times coordinated.[41] Given such a reality, framing the cyber domain as a complex social system, is both descriptively more accurate and also poses a framework in which to better unpack the relationships and interactions between security actors.

Assemblage thinking owes its intellectual roots to Giles Deleuze and Felix Guattari's book *A Thousand Plateaus* which developed an ontology that includes assemblages as a core entity in light of the development of a number of concepts including 'open systems, complexity, emerging and non-linear dynamics' in the global system.[42] For Deleuze and Guattari, an assemblage is a number of disparate and heterogeneous elements convoked together into a single discernible formation that displays some form of consistency and regularity while remaining open to transformative change, either through the addition or subtraction of elements, or the reorganisation of the relations between elements.[43]

Manuel DeLanda subsequently took the concept to develop a more comprehensive 'theory of assemblages'[44] that challenges existing social analyses – often focused at either an individual or societal level.[45] For DeLanda, the concept of assemblages should be used to analyse all social entities (from sub-individual to transnational) and therefore goes further than other scholars in proposing the term as a comprehensive ontology. In this regard, assemblages are

[41] ibid., 120.
[42] Giles Deleuze and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, (London: University of Minnesota Press, 1987).
[43] ibid., 502-505
[44] Manuel DeLanda, *Intensive Science and Virtual Philosophy*, (London, UK: Continuum, 2002); Manuel DeLanda, *A New Philosophy of Society: Assemblage Theory and Social Complexity*, (London, UK: Continuum, 2006); Manuel DeLanda, *Deleuze: History and Science*, (New York: Atropos, 2010).
[45] Oldrich Bures, *Private Security Companies*, (Basingstoke, UK: Palgrave Macmillan, 2015) 14.

not necessarily anything new or contingent on hybrid structures: even networks where the state is a highly dominant actor could be considered assemblages in their own right, according to DeLanda.

Assemblages have begun to be considered in an IR and security studies context too. In an analysis of shifting relationship between territory, authority and rights, Saskia Sassen has pushed back against the focus of globalisation literature on the withdrawal from the state in areas such as the economy as it often ignores the way states actively participate in setting up new structures.[46] Sassen goes on to suggest that modern global structures involve three key elements. First, a process of disassembly occurs where previously public functions are transferred to private actors. Second, in lieu of their new role, private actors develop their capacities in order to operate at the global level. Third, a process of 'reassembly' occurs where emerging private actors become part of global assemblages.[47] The key message being that particular components of the state are undergoing a process of reformation. In short, globalisation is not a matter of outside private forcers eroding state power and sovereignty; instead, it is a process entwined with a restructuring of institutions and power relations through practices such as privatisation and regulation.[48]

Abrahamsen and Williams were the first to apply assemblages to a security studies context by observing the emergence of private security companies in Africa.[49] Here, the concept of assemblages is used to examine the hybrid nature of security provision and to investigate processes of assembling and disassembling security in Africa.[50] For Abrahamsen and Williams, the concept of assemblages is very much a descriptive term. In discussing their work

[46] Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages*, (Princeton University Press, 2008).
[47] ibid., 21.
[48] ibid., 8.
[49] Rita Abrahamsen and Michael C Williams, "Security Beyond the State: Global Security Assemblages in International Politics."
[50] ibid.

Abrahamsen claims that they 'don't take much theoretical baggage with the term [assemblages] and I think that allows for a great deal of freedom.'[51] The concept of assemblages has also been deployed in a diverse range of security settings[52] including airports,[53] urban environments,[54] surveillance,[55] and resource extraction.[56]

Assemblage thinking now encompasses a broad church of thinking. As Michele Acuto and Simon Curtis put it, 'we can now legitimately talk of many styles of assemblage thinking – a feature that makes this approach less of a theory and more of a repository of methods and ontological stances.'[57] Within these different approaches lie debate and disagreement about the extent to which the concept should be used – much of which is captured in the edited volume *Reassembling International Theory* that includes contributions from a number of IR scholars that have used the term in their own work.[58] As previously discussed, for DeLanda, constructing assemblages provides the building blocks for an entire ontology or metaphysical system.[59] Likewise, although Olaf Cory acknowledges that the intellectual roots of assemblages are rooted in a scepticism of grand theory, he argues that the concept 'could be useful for re-thinking structure and models of structure in international relations.'[60]

---

[51] Rita Abrahamsen and Michael Williams., "Tracing Global Assemblages, Bringing Bourdieu to the Field: A Conversation with Rita Abrhamsen and Michael Williams," in *Reassembling International Theory*, (London, UK: Palgrave Macmillan UK, 2013), 25–31. pp. 26.
[52] Although much of this research sits outside of security studies and within disciplines such as critical geography and sociology.
[53] Randy Lippert and Daniel O'Connor, "Security Assemblages: Airport Security, Flexible Work, and Liberal Governance," *Alternatives* 28, no. 3 (2003): 351–58; Joakim Berndtsson and Maria Stern, "Private Security and the Public-Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage," *International Political Sociology* 5, no. 4 (December 5, 2011): 408–25.
[54] Abrahamsen and Williams, *Security Beyond the State*.
[55] Kevin D Haggerty and Richard V Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (December, 2003): 605–622.
[56] Rita Abrahamsen and Michael C Williams, "Security Beyond the State: Global Security Assemblages in International Politics,"; Abrahamsen and Williams, *Security Beyond the State*.
[57] Michele Acuto and Simon Curtis, "Assemblage Thinking and International Relations," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis (London, UK: Palgrave Macmillan UK, 2014), 1–15. pp. 2.
[58] Michele Acuto and Simon Curtis, eds., *Reassembling International Theory*, (London, UK: Palgrave Macmillan, 2013).
[59] ibid., pp. 6.
[60] Olaf Corry, "Global Assemblages and Structural Models of International Relations," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis, (London, UK: Palgrave Macmillan, 2013), 48-56.

Alternatively Stephen Collier has used assemblages to formulate an 'anthropology of the present.'[61] Collier has specifically criticised the 'empirical' movement in contemporary assemblage thinking on the grounds that it ought 'to "strategically focus on a few, consequential things" out of an infinite range of possibilities'.[62]

A second group of thinkers have pushed back on the extent to which the concept of assemblages should be used as part of a wider theory. Abrahamsen and Williams for instance see the term as more of a metaphor in order to examine the process of disassembly and assembly in security settings, in a claim that contrasts with Christian Beuger who claims that 'the way that assemblage is employed as a loose metaphor almost deprives it of any theoretical meaning.'[63] For Beuger, the concept of assemblages represents largely an empiricist project[64] claiming that the concepts provided by assemblage thinking 'should not be evaluated in how far they add up to an internally coherent theoretical apparatus but in the way they create space and open up new ways for the study of the international.'[65] Others such as Sassen and Aihwa Ong have also played down the extent to which the term provides scope for a wider theory of IR. Sassen argues that the term is more of an 'analytic tactic' that makes it possible to bring together components and parts of what are more conventionally considered as fully fledged institutions (such as governments, businesses, etc.). For Ong, using assemblages 'is not a theory:

pp. 49.

[61] Aihwa Ong and Stephen J Collier, *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, (Oxford, UK: Blackwell, 2005).

[62] Stephen J Collier, "Assemblages and the Conduct of Inquiry: a Conversation with Stephen J. Collier," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis (London, UK: Palgrave Macmillan UK, 2014) 32-38. pp 37.

[63] Christian Beuger, "Thinking Assemblages Methodologically: Some Rules of Thumb," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis, (London, UK: Palgrave Macmillan, 2013), 58–66.

[64] Oldřich Bureš, *Private Security Companies*: Transforming Politics and Security in the Czech Republic (London, UK: Palgrave Macmillan, 2015), pp 16.

[65] Christian Beuger, "Thinking Assemblages Methodologically: Some Rules of Thumb," 64.

assemblage is a way of framing our inquiry, to grasp perhaps critical interacting elements that would help us in analysing what is happening'.[66]

The approach of this thesis sits more closely to the second group of thinkers outlined above. Grander ontological arguments related more closely to the first group of assemblage thinkers are therefore avoided. Instead, the term provides a useful metaphor for capturing interesting cyber security processes that deserve more analysis. The assemblage concept serves a means in which to capture the network of actors that reside within a cyber security setting, understand their power and incentive structures; the dynamics and relationships that exist between security providers; and understand how this all affects security.

Assemblage thinking also represents a welcome contribution to broader critical theory in IR that challenges the traditional theoretical assumptions and language used in IR, (as opposed to Critical Theory with a capital C, which has grown out of Marxist traditions of social theory and is typically concerned with the emancipation of individuals).[67] Assemblage thinking sits as part of a long tradition of critical literature that aims to probe traditionally held concepts and institutions and in contrast to positivist or 'problem-solving' theories that often take such concepts for granted.[68] While various critical projects deserve praise for deconstructing and highlighting the limitations of the various concepts, they are often intellectually unsatisfying when alternative paradigms are not proposed to replace them (although such alternative conceptual approaches are not absent entirely). Security assemblage literature recognises this imbalance: it takes the limitations of traditional paradigms identified within critical security

[66] Saskia Sassen and Aihwa Ong, "The Carpenter and the Bricoleur: a Conversation with Saskia Sassen and Aihwa Ong," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis (London, UK: Palgrave Macmillan, 2013), 17–24. pp. 18-19.
[67] Karin M Fierke, *Critical Approaches to International Security* (Cambridge, UK: Polity Press, 2015) pp. 2.
[68] Robert W Cox, "Social Forces, States and World Orders: Beyond International Relations Theory," *Millennium* 10, no. 2 (June 1981): 126-155. pp. 128-129.

studies literature as a foundation, yet goes on to develop the concept of security assemblages as a means to move forward.

Various criticisms could be levelled towards assemblage approaches. At a most fundamental or first-order level, assemblage thinking could be criticised from a generic state-centric lens. The traditional notion of the state has served IR scholarship well for a long time – the concept has sustained despite a number of disruptions and technological revolutions in the international system. Yet, such a tired state-centric critique is becoming increasingly unhelpful and banal in the face of a variety of approaches that now acknowledge means for examining IR beyond state-centric viewpoints (such as notions of disaggregated sovereignty, actor-network theory, the military-industrial complex, etc.). The state is ultimately a dynamic term and one that holds a particular meaning within a specific historical structure.[69] Through engaging with world history, Barry Buzan and Richard Little have demonstrated that structural patterns vary considerably across time and space.[70] The system of states that has characterised much of IR theory should be seen as just one of many ways to characterise the world. An overview of world history shows that in the past, alternative units, such as tribes, empires, and city states, have more appropriately characterised the world.[71] The concepts used to capture reality are therefore open to interpretation. There are calls for IR scholars to consider the re-emergence of cities as important actors on the global stage and as part of emerging forms of global order for example.[72] The relativity of concepts means that thinking with assemblages should not be

[69] Barry Buzan and Richard Little, "Waltz and World History: the Paradox of Parsimony," *International Relations* 23, no. 3 (October 7, 2009): 446.
[70] ibid.
[71] ibid. 449; Charles Tilly, *Coercion, Capital and European States AD 990–1990,* (Oxford, UK: Basil Blackwell, 1990).
[72] Simon Curtis, "Cities and Global Governance: State Failure or a New Global Order?," *Millennium* 44, no. 3 (May 25, 2016): 455–77; Simon Curtis, *The Power of Cities in International Relations*. (New York: Routledge, 2014); Anni Kangas, "Global Cities, International Relations and the Fabrication of the World," *Global Society* 31, no. 4 (June 2017): 531–50.

particularly controversial – it is simply an alternative framework that is arguably more appropriate for studying diffuse cyber security structures.

If state-based security models are applied to the cyber domain, there is a danger that the private actors that possess the relevant security expertise will be side-lined in a way that undermines individual security. To discuss the state as the central provider of cyber security evokes, most clearly, neorealist paradigms. Yet, the traditional neorealist conception concerning the centrality of the state as the provider of security (regarded as a public good) for subjects (classified as citizens) against threats (external and predominantly in the form of other state militaries) that threaten due to the structural characteristics of the international system (namely, anarchy and the subsequent emergence of the security dilemma)[73] is a framework that does not apply to the same extent in cyber security contexts. When the source of threat and the means of security are misunderstood, the optimal provision of security becomes impossible to achieve. If preconceived notions should not be applied blindly, this thesis seeks to provide a richer understanding of the actors involved in providing security that may then offer insight for how security should be provided and by whom in order to create a secure cyberspace.

Public-private distinctions are also fluid, with areas such as public or private property perceived in fundamentally different ways between Ancient Greece and modern Western societies.[74] In his study of private military contractors, Peter W Singer determines that 'the public-private dichotomy…which was once solidly fixed, is now under siege.'[75] As well as ignoring the fact that states often make conscious decisions to use private actors, (often for strategic gain),[76] Owens points out that a number of these works fail to interrogate what is often a largely

[73] Keith Krause and Michael C Williams, "Broadening the Agenda of Security Studies: Politics and Methods," *Mershon International Studies Review* 40, no. 2 (1996): 229-254. pp. 232.
[74] Patricia Owens, "Distinctions, Distinctions: 'Public' and "Private" Force?," *International Affairs* 84, no. 5 (September 1, 2008): 977–90. pp. 981.
[75] Peter W Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, 8.
[76] Mumford, *Proxy Warfare;* Andrew Mumford, "Proxy Warfare and the Future of Conflict."

artificial distinction between public and private entities. While perhaps the primary mechanism for organising political, economic, and military power, the public-private distinction remains an ideological construct – albeit one rarely challenged.[77] As Owens stresses, 'there is no such thing as public or private violence. There is only violence that is made "public" and violence that is made "private."'[78]Global-local distinctions have likewise been probed by academics. Didier Bigo, for instance, has considered the implications of the rigid distinctions often drawn within security between the national constellation (characterised by crime, internal security, public order, and police investigations) and the international constellation (characterised by war, defence, international order and strategy).[79]

Ultimately, there is little benefit in dwelling on state-centric critiques any further. The IR discipline itself has moved on given the now rich menu of conceptual and theoretical tools available that can help to elucidate our understanding of contemporary security issues. Setting up, only to then knock down, state-centric approaches would make for an unhelpful straw man argument.

Moving beyond questions of the state, there remain substantive criticisms of the assemblage term that deserve careful consideration. It would be reasonable to criticise assemblage approaches for being overly descriptive for instance. This is not to say that such thick description projects do not have their place and indeed they can provide us with a level of nuance and insight that is difficult to come by through other approaches. Yet, the descriptive focus of many assemblage studies means that there are currently underexploited opportunities for assemblage thinking to go further: rather than just acknowledging diffuse and hybrid

[77] Patricia Owens, "Distinctions, Distinctions: 'Public' and "Private" Force?"
[78] ibid., 979.
[79] Didier Bigo, "Globalized (in)Security: the Field and the Ban-Opticon," in *Illiberal Practices of Liberal Regimes after 9/11,* ed. Didier Bigo and Anastassia Tsoukala (Abingdon, UK: Routledge, 2008), 10-48.

structures and the dynamics within these networks, but to also think what this means for security in more fundamental ways. Assemblage literature has proved capable of accounting for and observing interesting social structures, yet consideration of the key implications that arise from such a configuration of actors and entities can still be explored in more detail. The second chapter of this thesis proposes a theoretical model that enables assemblage thinking to provide more systemic and cohesive treatment in analysing contemporary security structures.

It could also be argued that many of the arguments associated with assemblage thinking go too far in embracing postmodernism. While traditional distinctions – between public and private, global and local, or state and non-state are often blurring, these categories remain useful categories to sort and organise reality. While the government and private sector may often become increasingly embedded with one another, this does not mean it is wholly incoherent to refer to the government or private sector entities. While rigid and binary concepts should not restrict our understanding of emerging structures and practices that transcend and intersect them, assemblage thinking should conversely be careful in dismissing conventional terms too readily. Assemblage thinking therefore deserves credit for acknowledges hybridity and the way in which actors can become embedded and amalgamated with one another in a way that the ontological distinctions between different actors become increasingly blurry. Yet, while a welcome development, it is also important to delineate between and within security structures. When drawing an assemblage, some areas will naturally be more hybrid than others. Hybridity is therefore more appropriately framed as an important variable to consider, rather than an endemic feature of assemblages. The theoretical model in Chapter Two will therefore articulate assemblage fusion as a component of an assemblage's dynamic – and crucially a variable that has an influential bearing on the security outputs that arise from security structures.

Cyber Security Assemblages

IR and security studies now have a rich intellectual history of questioning the traditional definitions, concepts, and distinctions used to capture the international system. Literature using the assemblage term deserves credit for providing a compelling alternative that overcomes some of the weaknesses associated with more traditional approaches. Thinking with assemblages not only provides a descriptively rich and nuanced account of security provision, but also offers currently underexploited opportunities to understand the implications that arise from the security entities, and the relationships between entities, that exist within contemporary security structures.

Nowhere is the application of these issues as relevant than in the context of cyber security.

The assemblage term is used in this thesis given the concept's ability to articulate and capture key processes of cyber security provision that have so far been under analysed: the diffuse network of security providers; the often hybrid nature of security structures; the diachronic and unstable process of security provision as actors and their capabilities shift over time; the often contested nature of security given the variety of motivations exhibited; etc. An assemblage approach puts these processes at the centre of its analysis, making it possible to understand how they drive cyber insecurity.

Various cyber security contexts contain a complex constellation of actors that reinforce the reasoning behind approaching cyber security provision through an assemblage lens. The protection of CNI provides a case in point with the notion of security as a public good and the idea that the security provision can be separated clearly between public and private actors problematic. There is a muddled view of who is responsible for the cyber security of the infrastructure in both the UK and US where CNI has been largely privatised. Governments have previously made it clear that the protection of privately owned CNI from cyber attacks is

not a governmental responsibility.[80] For example, despite calls from the US banking sector for the US government to respond to an Iranian cyber attack on US banks, the White House remained reluctant to intervene.[81] Likewise, there is a clear absence of any central point of control or of laws that require operators of CNI to conform to minimum security standard within the UK.[82] Yet, even when governments have distanced themselves, the protection of critical national infrastructure is not entirely outside their purview. While UK government organisations do not provide hands on support in a crisis, various government actors nevertheless provide a range of supporting functions including risk assessments, the auditing of security arrangements and the provision of vulnerability reports.[83] Further, in March 2016, the UK Government Communications Headquarters (GCHQ) intervened to secure a new system of smart energy meters, after discovering a vulnerability that would allow a malicious actor to threaten the supply of gas and electricity for millions of UK citizens.[84] In the protection of CNI , there is therefore a clear tension: on the one hand, government actors are reluctant to take on responsibility for the issue (given the negative repercussions if a breach or compromise occurred);[85] at the same time, they also fear that the private owners of CNI will not be appropriately incentivised to provide an adequate level of security for end-users without government intervention.[86] The protection of CNI therefore comprises a more complex security assemblage that includes both public and private organisations with the interests of these actors

[80] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies."
[81] Rob Knake, "Obama's Cyberdoctrine: Digital Security and the Private Sector," *Foreign Affairs*, May 6, 2016, https://www.foreignaffairs.com/print/1117450.
[82] Warwick Ashford, "Is UK Critical National Infrastructure Properly Protected?," *Computer Weekly*, March 3, 2011, http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.
[83] Jamie Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," in *Ethics and Policies for Cyber Operations*, Philosophical Studies Series (Cham, Switzerland: Springer, 2017), 187–212.
[84] Pilita Clark, "GCHQ Intervenes to Secure Smart Meters Against Hackers," *Financial Times*, March 18, 2016, https://next.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8.
[85] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies."
[86] "National Cyber Security Strategy 2016-2021" (HM Government, November 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdfhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

both converging and competing. As argued by Lene Hansen and Helen Nissenbaum, 'cyber security is not left to the liberal market, but implies a complex constellation of public-private responsibility and governmental authority.'[87]

Likewise, an examination of security actors involved in encryption illustrates an equally complex assemblage of security actors. More interesting still, is the asymmetry of power and authority among public and private actors. In February 2016, Apple refused a Federal Bureau of Investigation (FBI) request to unlock an iPhone connected to a mass shooting in order to protect the privacy of its customers from state intrusion – the very actor that mainstream theorists would regard as the primary guarantor of national security. Although the shooting first appeared largely insignificant and removed from a broader IR perspective, the case soon became wrapped into a broader debate about the trade-off between privacy and security which had much broader security and philosophical implications. In the Apple-FBI dispute, multiple and opposing forms of security clashed: the FBI's desire for potential intelligence that could prevent other shootings conflicted with Apple's business interests and desire to protect the privacy of its global customer base.[88] Further, specific organisations within public and private spheres possess their own distinct agency and incentive structures; categorising all private or public actors as uniform is therefore inaccurate. Consider that it was a private actor that eventually unlocked the iPhone in question with the task outsourced to Israeli firm Cellebrite, also demonstrating that the security assemblage within the encryption field comprises a variety of agents that are both local and global.[89] Further, the National Security Agency (NSA) – the organisation that likely instigated the encryption of Apple devices in the first place[90] – remained

[87] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," 1162.
[88] Harold Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (November 17, 2015): 69–79.
[89] Tova Cohen, "Israeli Firm Helping FBI to Open Encrypted iPhone: Report," *Reuters*, March 23, 2016, http://www.reuters.com/article/us-apple-encryption-cellebrite-idUSKCN0WP17J.
[90] In response to the revelations within sensitive NSA documents leaked by Edward Snowden

reluctant to assist the FBI in unlocking the device due to different organisational cultures and objectives.[91] This shows the difference between various government actors. Turning to the UK public sector, while Apple has publicly resisted the UK government's attempt to access the communication of Apple customers,[92] the technology firm has simultaneously benefitted from information provided directly by GCHQ related to exploits of its software and devices in order to improve their security,[93] again showing the multifaceted dynamics of relationships between actors.

It has become increasingly untenable to doubt the importance of cyber security to high politics and IR. Rather than abstract theoretical propositions, it is empirical realities that make this the case. A range of cyber attacks and incidents are increasingly showing the very real threats that exist within the domain. Solutions cannot be meaningfully addressed if problems are not first identified and understood. By understanding the drivers of cyber insecurity, it then becomes possible to develop solutions to the problems identified. This thesis contends that issues related to security provision, and the diffuse nature of security provision caused by the emergence of non-traditional actors represent key, yet underestimated, drivers of cyber insecurity. Thinking with assemblages makes it possible to further explore these issues.

Cyber security literature has already made encouraging progress in addressing many of the issues associated with security provision and the emergence of non-traditional actors.

[91] Russell Brandom, "Why the NSA Is Staying Out of Apple's Fight with the FBI," *The Verge*, March 9, 2016, http://www.theverge.com/2016/3/9/11186868/apple-fbi-nsa-encryption-exploit-hack.
[92] For example, in late 2015, Apple called on the UK Government to change its Investigatory Powers Bill arguing that it would weaken security and privacy. See Alex Hurn, "Apple Calls on UK Government to Scale Back Snooper's Charter," *The Guardian*, May 21, 2015, https://www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill.
[93] Joseph Cox, "GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS," *Motherboard*, April 29, 2016, http://motherboard.vice.com/read/gchq-vulnerabilities-mozilla-apple.

The empowerment of non-state actors has been noted as a key characteristic of the cyber domain. In *The Future of Power*, while it is recognised that states remain powerful actors, Nye explains how a process of 'power diffusion' has occurred within the cyber domain due to low costs and barriers to entry. This has empowered individuals and private organisations, ranging from corporations to non-governmental organisations (NGOs) to terrorist cells and enabled them to play direct roles in world politics. This spread of information means that power is more widely distributed and informal networks will increasingly replace traditional bureaucracies.[94] Furthermore, given that barriers to entry are particularly low, non-state actors are able to easily exit and re-enter the cyber domain, affording them a greater flexibility and adaptability when compared to states.[95]

Yet, the majority of analysis has considered how power diffusion leads to emerging threats, rather than emerging security providers. The threats that arise from non-traditional actors has therefore gained a great deal of interest. Gregory Rattray and Jason Healey have made a compelling case for the strategic effects of non-state actors to be taken seriously. They explain how private actors possess advanced capabilities in relation to offensive cyber tools[96] that are typically sold, either to states through direct cooperation as well as increasingly through online underground markets. Indeed, markets for cybercrime tools are increasingly growing in sophistication.[97] The strategic effect of private actors is further demonstrated through the alliances that they forge: states often conduct aggressive operations via private actors in order to distance themselves from such actions and muddle attribution.[98] Rattray and Healey have also captured the spirit of assemblage thinking when they argue that 'to address the challenges

[94] Joseph S Nye Jr, *The Future of Power*, (New York: Public Affairs, 2011) 115-116.
[95] ibid., 115.
[96] This includes knowledge of vulnerabilities and exploits of systems. Such knowledge is not an offensive tool per se but can nonetheless be used for offensive purposes.
[97] Lillian Ablon, Martin C Libicki, and Andrea A Golay, "Markets for Cybercrime Tools and Stolen Data; Hackers' Bazaar" (RAND, March 2014).
[98] Gregory J Rattray and Jason Healey, "Non-State Actors and Cyber Conflict," 72-73.

and opportunities presented by the dominance of non-state activity in cyber conflict, it is essential to approach the cyber domain as an ecosystem of competing and collaborating actors.'[99] Given the dominance of private actors, they argue that collaboration between public and private actors is instrumental.[100]

In the context of discussing the disruptive effects of the cyber domain on mechanisms of world politics, Kello discusses the ability of private actors to inflict economic and social harm citing the Georgian cyber attack in 2008 as a case in point. The Georgian attacks, conducted by Russian criminal groups, crippled the government's communications infrastructures in addition to paralysing the operations of the National Bank of Georgia which impeded the procurement of essential war materials. Ultimately, the use of non-state actors meant that the Russian military was not directly implicated in the attack.[101] In addition, non-state parties are not usually considered subjects of international law and thus not subject to its penalties.[102] As Kello mentions when considering cyber conflict, as well as considering traditional state-to-state conflict, it is also necessary to consider private-to-private, state-to-private and private-to-state conflict.

Reversing the consideration of power diffusion to explore security provision (rather than threats) is comparatively under analysed, yet literature in this area has already made encouraging progress. A variety of academics have considered the implications that arise from security providers.

Studies that have considered the multiple securities that exist in cyber security have made an important contribution in showing the implications that arise from security structures that

[99] ibid., 68.
[100] ibid., 67.
[101] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."
[102] ibid., 25.

comprise multiple entities. Ronald Deibert, for instance, has considered how since its beginnings, the internet's architecture has been built 'not only by states and corporations but also by the distributed base of users themselves.'[103] The resources of these millions of users spread around the world should not be underestimated. In bringing such civic networks into the picture, Deibert has demonstrated that power relations comprise highly complex and transnational networks. This point was exemplified in Deibert's earlier work that emphasises the multiple security discourses that occur within cyber security contexts.[104] Deibert has also discussed how technology firms are increasingly becoming deeply political actors.[105] Likewise, Lene Hansen and Helen Nissenbaum have highlighted that within cyber security, referent objects other than the state are threatened – notably individuals.[106] Literature associated with the Copenhagen School deserves credit for focusing on the multiple securities that often exist, and the way in which a government's incentives do not necessarily correlate with that of individuals.[107] Hansen and Nissenbaum cite a RAND gaming exercise that included a range of cyber attacks on critical national infrastructure and financial systems.[108] As they point out, the RAND scenario highlighted how 'cyber security discourse moves seamlessly across distinctions normally deemed crucial to Security Studies: between individual and collective security, between public authorities and private institutions, and between economic and political-military security'.[109] Hansen and Nissenbaum note that governments are keen to hold private sector firms 'co-responsible for cyber security' in order to spread the financial and

[103] Ronald J Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," 527.
[104] Deibert, Ronald J, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, ed. James N. Rosenau and JP Singh (Albany, GA: State University of New York Press, 2002), 115-142.
[105] Ronald J Deibert, *Black Code: Inside the Battle for Cyberspace*, 94-97.
[106] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," 1160.
[107] Barry Buzan, *People, States & Fear*, (Colchester, UK: ECPR Press, 2016); Karin Marie Fierke, *Critical Approaches to International Security* (Cambridge, UK: Polity Press, 2015).
[108] Robert H Anderson and Anthony C Hearn, "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA 'the Day After...in Cyberspace II'," (RAND, 1996).
[109] ibid., 1161

political burden amongst a range of actors.[110] Yet, private actors have simultaneously called for states to strengthen intellectual property rights and to be vigilant in prosecuting cyber crimes. Ultimately, this means that 'negotiation of the boundaries between the public and the private and between the economic and the political thus couples the network-fragmentation implied by "cyber."'[111]

It is therefore vital to understand the implications that arise from such complex configurations of security providers. Adverse incentives often distort the nature of cyber security provided. Myriam Dunn Cavelty, for instance, has explained how cyber security is regularly militarised, creating an unnecessary atmosphere of insecurity and tension in the international system and focuses the issue on national security measures, rather than economic and business solutions.[112]

Whilst public-private partnerships have been presented as an essential characteristic of national cyber security strategy,[113] the dysfunctional aspects of these arrangements deserve serious consideration. Cavelty and Manuel Suter have highlighted the limitations of public-private partnership models in the protection of CNI, with such arraignment more appropriate for maximising efficiency rather than enhancing security.[114] Cavelty and Suter therefore called for a new understanding of the role of the state in CNI protection, moving away from monitoring actors that collaborate with it, but rather co coordinate and stimulate functional networks, based more in line with the notion of self-regulating networks.[115] The limitations of public-private

[110] ibid., 1162
[111] ibid., 1162
[112] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better"; Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension."
[113] Arnav Jagasia, "A Look into Public Private Partnerships for Cybersecurity," Public Policy Initiative, University of Pennsylvania, April 18, 2017, https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for; William J Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September 2010): 97–108.
[114] This argument was made in relation to security provision more generally and therefore not restricted to cyber security specifically. See, Myriam Dunn Cavelty and Manuel Suter, "Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection."
[115] ibid., 183-186.

partnerships have also been noted in a cyber security context specifically. Madeline Carr for instance has shown that both public and private institutions are averse to accepting greater responsibility or liability for national cyber security, leaving partnership arrangements often ambiguous and with responsibility and accountability over national infrastructure left ill defined.[116] Carr also questioned neoliberal arguments that advocate security investments being determined by the market, with private firms' cost-benefit analyses often failing to fully accommodate the public interest[117] – a sentiment also echoed by other thinkers.[118] Carr has also argued convincingly that multi-stakeholder governance approaches to the internet have also enabled dominant states and private firms to exert a disproportional amount of power and influence.[119]

Progress on understanding diffusion has also been made at a more conceptual level. Thierry Balzacq and Cavelty, for instance, examined cyber security and malware via actor network theory arguing that a 'regional topography has shaped IR imagination for a long time and in particular through the invention and institutionalisation of borders and sovereignty.'[120] They instead favour actor network theory given its ability to establish relationships between elements that are distant in geographical terms. As they argue, 'the localisation of objects does not determine their proximity'.[121] Florian Egloff has also argued that the rigid public-private

[116] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies."
[117] ibid.. 60.
[118] Judith H Germano, "Cybersecurity Partnerships: A New Era of Public-Private Collaboration" (The Center on Law and Security, NYU School of Law, October 2014), http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.
[119] Madeline Carr, "Power Plays in Global Internet Governance."
[120] Thierry Balzacq and Myriam Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security," *European Journal of International Security*, May 12, 2016, 1–23.
[121] ibid., 11.

distinctions used to describe actors in the cyber domain are inappropriate given the presence of many actors that exist in between these two concepts – forms of semi-state actors.[122]

The above literature has therefore made a number of important contributions in highlighting both the existence of diffuse security structures, and the implications that arise from it. This thesis seeks to further develop this body of literature by exploring security provision through an assemblage lens. Whether it is certain phenomena (such as securitisation or militarisation) or specific types of relationships (such as public-private partnerships or multi-stakeholder approaches), current literature has often focused on certain trends of security provision in depth. This has been a welcome development, and it is often necessary to explore such issues in isolation in order to develop a deep understanding of them. Yet, the complexity of contemporary cyber security structures means that many of these trends and processes are occurring simultaneously. An assemblage approach therefore acknowledges the developments others have discussed and seeks to provide a more overarching conceptual framework that can account for multiple phenomena (whether that be clashing securities, securitisation, divergent incentive structures, etc.) in a more cohesive and holistic manner.

Applying assemblage thinking to cyber security therefore makes both theoretical and empirical contributions. From a theoretical standpoint, this thesis seeks to further develop literature that connects issues of security provision to cyber insecurity. Based on the above review, existing literature might be grouped into three camps that seek to understand drivers of cyber insecurity: the dysfunctional nature of cyber security provision; the complexity or scale of the threat surface; and the structural factors inherent to the domain. All three of these issues deserve consideration together. Yet, while each of these three concerns are valid, there remain open

[122] Florian Egloff, "State, Semi-State, and Non-State Actors in Cybersecurity," (Understanding Change in World Politics nternational Studies Association 58th Annual Convention, Baltimore, MA, February 22-25, 2017).

questions related to the weighted importance of each. This thesis argues that not enough attention has been placed on issues of security provision, while aspects of the other two drivers have at times been exaggerated. A central ambition of this thesis is to therefore make the case for why issues related to security provision matter – by further developing empirical evidence through an assemblage approach that highlights how the security providers, and the dynamics between security providers, have a crucial bearing on the nature of cyber security. In addition to building on cyber security literature, this thesis also seeks to show how assemblage thinking can be used to understand the security implications that arise from complex security structures (as opposed to a tool primarily concerned with describing and observing). This aspect of assemblage theoretical building is developed in Chapter Two, with the assemblage theoretical model presented providing a conceptual framework used in the empirical case study chapters.

The core empirical contribution of this thesis will be in identifying and clarifying the makeup and configuration of actors within the cyber domain, drawing on three case studies. As is to be expected with a nascent security issue, a variety of organisations have clamoured to capture cyber security remits in an attempt to bolster their mandate. For example, NATO officials have sought to label the cyber domain as the 'fifth domain of warfare' in a move that clearly militarises the issue while the EU has typically framed cyber security through its own projects (such as in the context of the Digital Single Market).[123] Here, an assemblage approach presents an understanding of the configuration of security actors that facilitates a more productive consideration of security. This is particularly useful when there are instances of clashing securities. Critical thinkers have previously argued that the term security is itself an 'essentially contested concept'.[124] As the Apple-FBI encryption dispute outlined in Chapter Three will

[123] "Digital Agenda Scoreboard Key Indicators," European Commission Digital Single Market, accessed April 23, 2018, https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/visualizations.
[124] Walter B Gallie, "Essentially Contested Concepts," *Proceedings of the Aristotelian Society* 56, (1956): 167–98.

show, actors hold varied, and sometimes opposing, security objectives. The empirical contribution of this thesis intends to unearth the incentives of various actors and the implications this has for security. For example, in 2011, the UK government assumed that private owners of CNI would implement effective cyber security protocols independently, motivated solely by market mechanisms. The 2010 Cyber Security Strategy had previously emphasised a hands-off approach, regarding regulation as a blunt instrument.[125] However, it has since been acknowledged that a market failure exists and private firms are not suitably incentivised by market mechanisms that have led to a rethink within government circles.[126] Such a reversal in policy demonstrates that understanding the incentives of different actors is crucial. If market failures do exist in a private-dominant domain, then state intervention may be welcomed. Conversely, other case studies may show that states actions are prioritising state interests over individual security (as is arguably the case in ongoing encryption debates within the US for example).

With the role of the state as the primary security provider under question, the findings of this thesis are, by definition, relevant to policymakers. Public organisations are clearly not the sole provider of security in the cyber domain; yet they must still grasp the issue. For a start, public organisations need to protect much of their own infrastructure. If governments do not possess the internal capability to secure their own systems, there is an immediate need to work with other actors which leads to its own challenges in managing issues such as outsourcing, vetting, and supply chain procedures. By outlining the configuration of specific security topics, it is

[125] "The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World" (The Cabinet Office, November 2011), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[126] Sam Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," *Financial Times*, November 9, 2015, https://next.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896; Tom Reeve, "Industry's Cyber-Security "Market Failure" Must Be Addressed," *SC Magazine*, May 23, 2016, http://www.scmagazineuk.com/industrys-cyber-security-market-failure-must-be-addressed/article/498249/.

hoped that policymakers will have a better idea on both how to secure both their own infrastructure, and assist other actors when required.

These issues are also important for private actors. Private sector firms are increasingly participating in the political processes related to cyber security. Technology and cyber security firms are increasingly wading into foreign policy and ethical challenges previously outside their purview. These firms will have to decide if, and to which governments, they supply their data for the purposes of national intelligence – a particularly thorny issue when it is unclear whether a state intends to use such data to genuinely protect citizens and improve security, or in fact, be used by leaders to tighten their grip on power and suffocate dissent.

These issues also affect individuals. In the post-Cold War period, critical security studies thinkers increasingly question the traditional notion of security, tied to states and the military, and began to further explore the notion of individual security.[127] Security is also a subjective and even 'essentially contested concept.' The idea of a contested concept was initially proposed by Walter B Callie who claimed a concept is contested when it is not just difficult to agree on a definition, but when a definition is disputed given that all definitions are theory-dependent and contain normative commitments.[128] Issues within cyber security such as encryption unearth conflicting security objectives amongst different actors. This means that the interests of a government or a private sector firm do not necessarily reflect that of individuals. In the case of technology firms, they may publicly guard their users' privacy by refusing to work with governments, yet readily monetise sensitive user data for the purposes of advertising.[129] Such a contradiction shows that these actors are in fact motivated by business and economic interests

[127] Karin M Fierke, *Critical Approaches to International Security* (Cambridge, UK: Polity Press, 2015) pp. 20-31.
[128] Gallie, "Essentially Contested Concepts."
[129] John Naughton, "Google, Not GCHQ, Is the Truly Chilling Spy Network," The Guardian, June 18, 2017, https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network.

related to the preservation of their reputation and brand. Debate therefore needs to follow on where the balance between different forms of security should lie when they affect individuals. For this to occur, an appreciation of what these tensions are, the incentives of various groups, and the specific actors that provide security are all required Despite the variety of actors involved in the provision of cyber security, cyber security assemblages regularly lack actors or institutions that truly represent civil society constituencies.[130]

Methods

A case study approach is the most suitable method to analyse cyber security assemblages given its ability to provide a rich and meaningful understanding of the configuration of security actors. The three topics studied in this thesis – CNI, encryption and digital society – all contain complex social phenomena that require extensive and in-depth exploration. Ultimately, to understand the configuration of security actors, it is necessary to study cases and events that unearth security practices and show how security is provided, and by which actors. Previous cyber security incidents have often shown that *ad hoc* responses can supersede formal plans and strategies. For example, while government institutions were primarily responsible for protecting critical infrastructure in Estonia, a number of volunteers formed a spontaneous civilian defence response in the face of a serious Russian directed attack in 2007.[131] Such divergence between intentions and actual practices makes the study of cases crucial. Although case studies are often used in order to infer causal mechanisms, this is not their sole purpose: in this thesis they are used to provide a rich understanding of phenomena that addresses the core research question at hand.

[130] Madeline Carr, "Power Plays in Global Internet Governance."
[131] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom."

A case study approach offers several advantages. They provide what Clifford Geertz referred to as 'thick description', where the broader context of a case is articulated, making the case more meaningful to outsiders.[132] Case studies are also a useful tool for studying unusual phenomena. According to Robert Stake, a case study is defined by an interest in an individual case, rather than the methods of inquiry used given that the object of study is itself a 'specific, unique, bounded system.'[133] The case study method makes detailed analysis possible and is able to retain the holistic and meaningful characteristics of the real-life events that are crucial for informing the findings of this thesis.[134] A case study's ability to accommodate complexity is therefore its most compelling feature. Andrew Bennett and Colin Elman reinforced this point when they argued that the use of case studies is ideal for studying the formation of new international security systems that 'often involve interaction effects among many structural and agent-based variables, path dependencies, and strategic interaction among large numbers of actors across multiple levels of analysis.'[135] They go on to argue that case studies, as well as other qualitative methods have been prominent in IR given their ability to study 'complex and relatively unstructured and infrequent phenomena that lie at the heart of the subfield.'[136]

Case studies have been deployed in a variety of ways within IR, from pure description to establishing causal mechanisms.[137] For the purposes of this thesis, an ideographic type of research is pursued. This means that facts are allowed to speak for themselves (rather than funnelled through a top-down theory) with their significance brought out through intuitive

[132] Clifford Geertz, *The Interpretation of Cultures* (New York: Basic Books 1973).
[133] Robert E Stake, "Qualitative Case Studies," in *Strategies of Qualitative Inquiry*, ed. Norman K Denzin and Yvonna S Lincoln, (Thousand Oaks, CA, SAGE Publications, 2008), 119-150; Ben Willis, "The Advantages and Limitations of Single Case Study Analysis," *E-International Relations*, July 5, 2014, http://www.e-ir.info/2014/07/05/the-advantages-and-limitations-of-single-case-study-analysis/.
[134] Robert K Yin, *Case Study Research: Design and Methods*, 4th ed., (Thousand Oaks, CA: SAGE, 2009) 4.
[135] Andrew Bennett and Colin Elman, "Case Study Methods in the International Relations Subfield," *Comparative Political Studies* 40, no. 2 (June 30, 2007): 170-195. pp. 171.
[136] ibid 79.
[137] Roger Gomm, Martyn Hammersley, and Peter Foster, eds., *Case Study Method*, (London: SAGE Publications, 2000).

interpretation.[138] An ideographic approach contrasts with a nomothetic research design, that seeks to make generalisations and develop rules that have been popular in IR literature[139] and within case study research specifically.[140] The case studies in this thesis also contain a configurative element with an ambition to depict the overall configuration of security actors in a particular context. Together, these two features combine to produce a configurative-idiographic study – a term proposed by Harry Eckstein.[141]

Various assumptions accompany a configurative-idiographic case study. In studying the configuration of security actors, there is no attempt to attain prediction and the level of control found in a natural-science approach.[142] Instead, emphasis is placed on understanding the context of the cases studied – although this may lead to some form of non-deductive conceptions of possible futures. Second, there is a subjective aspect of research given the interpretative approach in this thesis. This means there is a degree to which details are lost or at least distorted in abstraction and analysis as the security assemblages studied in this thesis are interpreted.

A configurative-idiographic approach has the benefit of providing a rich insight into the case studies at hand. Intuitive interpretations provide a nuanced understanding of the configuration of security actors. The case studies therefore offer a useful discussion of what security looks like, which actors provide it and where power lies in a deeper way when compared to other approaches. This is particularly important given the limitations of previous approaches in

[138] Harry Eckstein, "Case Study and Theory in Political Science," in *Case Study Method*, ed. Roger Gomm, Martyn Hammersley, and Peter Foster, (London, UK: SAGE Publications, 2000): 119-164.
[139] Gary King et al, *Designing Social Inquiry*.
[140] Robert K Yin, *Case Study Reseach: Design and Methods*.
[141] Eckstein, "Case Study and Theory in Political Science."
[142] ibid.

regard to the language, theories and concepts used to articulate security actors and security formation.

Academics have criticised configurative-idiographic case study approaches. Sidney Verba has argued that they 'do not add up very easily' given that they fail to produce reliable and valid statements of regularity about sets of cases.[143] It might be argued that the interpreter of such a case study simply considers a body of observations that are not self-explanatory. Further, without hard rules of interpretation, any number of patterns could be discerned that are more or less plausible.[144] Yet, such criticism is mitigated given that a configurative-idiographic case study does not claim to produce the generalisations or rules related to causal mechanisms associated with more positivist projects.[145] Where the debate should lie, therefore, is in much more fundamental first-order epistemological issues – in regards to whether such interpretive approaches are even plausible or useful. Here, the arguments outlined by Patrick Jackson offer a helpful way forward, where he suggested that various epistemologies can co-exist, with different approaches all capable of making a useful contribution in their own way.[146] In this regard, case studies that follow a more positivist approach should not necessarily be dismissed – they just produce a different form of knowledge.

Moreover, aspects of positivist case study research design can still provide a useful guideline for research. For example, Yin outlines four tests that determine the quality of empirical social research. While some of these rules relate purely to causal case studies, aspects can still be usefully applied in order to produce more robust interpretive case studies. For example, whilst Yin has suggested that case studies should be free from subjective judgements, (something an

[143] Sidney Verba, "Some Dilemmas in Comparative Research," *World Politics* 20, no. 1 (October 1967): 111-127. pp. 112.
[144] ibid.
[145] ibid.
[146] Jackson, *The Conduct of Inquiry in International Relations*.

idiographic approach instead embraces), it is possible to take Yin's suggestion to use multiple sources of evidence as a means to partially ground the inherent biases and subjective judgements inherent in research. While this is not carried out with the agenda Yin intended (i.e. to prevent subjective judgements entirely), it at least ensures that subjective judgements are fairer and more reasonable. Likewise, Yin argues that cases should be reliable so that if another investigator followed the same procedures in the same case studies chosen in this thesis, they would reach the same findings and conclusions. This means that errors and possible bias should be minimised as much as possible.[147] Again, while an idiographic approach that acknowledges research has an interpretive element and would push back against attempts for case study research that can be replicable in this form, it does not mean that Yin's advice for how to achieve reliable research should be dismissed. Reliable case studies involve a clear documentation of the procedures followed within a case study. This involves being transparent with how data is being collected and how it feeds into case studies. A clear record of the questions being asked in interviews and the appropriate citation of sources are both therefore crucial. Given the clandestine and classified aspects of cyber security, it will be mentioned when the answers to relevant question are unknown or where relevant data is confidential.

Case studies have been chosen based on their viability from a research standpoint. An initial examination has shown that data is publicly available on the three topics of this thesis. As an author, I also have an initial research network and base-level knowledge on the three topics that will make searching for relevant documents and secondary literature or arranging interviews more straightforward when compared to other topics. Other equally important cyber security issues – internet governance and cybercrime being the most obvious examples – also warrant further research. Examining these other topics with an assemblage approach would be

[147] Yin, *Case Study Research: Design and Methods*, 45.

undoubtedly relevant and useful (given that security practices in these topics also cross public-private and global-local distinctions). Time and resource constraints make it unviable to cover these important topics. However, it is intended that the work in this thesis will make a strong case for examining the cyber domain with an assemblage approach that will lay the foundation for future research in these other areas.

The three cases in this thesis are on different topics and within different countries. This clearly limits the generalisability of the insights found (an ambition not prioritised within idiographic research anyway). If the three case studies were all based on encryption, or all based on the UK context, for example, then it would be possible to make more substantive arguments about, say the issue of encryption or cyber security in the UK. Yet, while a deviant case selection limits the ability to test causal processes, it brings a value for new and more exploratory forms of research.[148] There is, therefore, a motivation to look at contrasting cases deliberately in order to appreciate the depth and variety of examples.

If not the topic or the country, the consistent theme that binds the three case studies is the diffuse characteristics of the security structures. In all three cases, there is a variety of actors involved in the security assemblage. The emphasis of this thesis is on understanding the implications of diffuse cyber security structures. It is therefore the configuration of security actors and the dynamics that exist within the security assemblages that represent the most significant variables.

The topic of cyber security remains poorly developed for many countries. There is little benefit in looking at a number of government's cyber security policies (or the configuration of cyber security actors) if it is an issue that has not reached an appropriate level of maturity. Part of the

[148] Jason Seawright and John Gerring, "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options," *Political Research Quarterly* 61, no. 2 (2008): 294–308. pp. 302.

rationale of selecting the three cases of this thesis therefore is based on identifying cyber security assemblages that are highly advanced or developed. In no other country is the concept of digital society as clearly developed as it is in Estonia. Encryption disputes between public and private actors are most contentious in the US. The constellation of actors in the UK critical national infrastructure assemblage are some of the most diverse globally. Whilst the disparity of cases and the idiographic-configurative approach as discussed above mean that generalisable claims found in this thesis are limited, there is nonetheless an advantage in looking at the most advanced case study within a particular security context. By understanding how a security topic has developed within a context that is highly advanced, it is possible to at least outline the realms of possibility for other countries that are yet to meaningfully confront these issues. For example, whilst the configuration of security actors responsible for providing cyber security for UK critical national infrastructure may not be directly applicable to other contexts, the insights yielded in this thesis will nonetheless provide useful takeaways for other market economies and countries with significant private ownership of critical national infrastructure assets. This is because these similar dynamics across countries could pose similar security implications. This means that despite the variety of cases studied, this thesis is still able to produce generalisable arguments related to the security of specific referent objects. These finding can be applied to other assemblages not studied directly.

There is also a pragmatic element to the case selection. Access to publicly-available data, my own network of researchers and practitioners, and the accessibility of the three cases make them viable from a research point of view. Studying the UK context made sense given that I am based in the UK and have a ready access of contacts familiar with the issue at hand. Given the extent of public debate surrounding the issue of encryption in the US, there are plenty of available public documents that can be analysed. I was also able to spend six months in the US during my research based at the Massachusetts Institute of Technology (MIT) as a Cyber

Security Fulbright Scholar. In the early stages of my doctorate, I worked as an intern in Estonia at the NATO Cooperative Cyber Defence Centre of Excellence and have also returned to Estonia multiple times to both teach and to assist with research on various aspects of the Estonian digital government initiatives that have helped me to understand Estonia's digital society.

Interviews formed the primary data collection method used. The main aim of conducting interviews was to speak to individuals working directly for security providers, and those who were security providers themselves. This involved speaking to government officials, technology firm employees, and cyber security consultants for example. This made it possible to gain an in-depth understanding of the security providers' characteristics and essential makeup.

In order to maximise the insights of this thesis, subject matter experts on the case study topics were also interviewed. Although these were not security providers per se, interviewing experts (including academics and think tank researchers) meant that this thesis was able to benefit from the insight of those with a deep understanding of the issues at hand. Often, these experts had good connections with security providers, and were therefore able to provide a rich insight on the characteristics and dynamics of relevant actors. With individuals working directly for security providers also likely reluctant to criticize their employer, speaking with third-party experts also provided a more candid discussion at times.

Participants were interviewed for a short period of time (between 30 to 60 minutes) with discussions remaining open ended and of a conversational manner – but nonetheless following a certain set of questions.[149] Questions were focused on the central research question of this

[149] Robert K Merton, Majorie Fiske, and Patricia L Kendall, *The Focused Interview: A Manual of Problems and Procedures*, (New York: Free Press, 1990).

thesis, seeking to gain an understanding of both security providers themselves (including their incentive structures and capabilities) as well as how security providers interacted with one another within the broader assemblage studied. Where possible, interviews took place in person to encourage a more open and candid discussion,[150] although some interviews were conducted via Skype when this was not possible.

Relying on interviews exclusively, however, would provide only limited insight – despite interviewees being helpful, generous with their time, and experienced in the issues examined in this thesis. Human participants come to interviews with their own prejudices and agendas.[151] This applies both on the part of participants but also on my own position as an author. Interviews come with a set of challenges, including making sure that they do not just substantiate preconceived positions. There is also a risk of 'snowballing' with many of the interviews conducted based on personal connections and referrals (potentially leading to an overly narrow and distorted perspective.[152] Likewise, it was important to consider the biases of interviewees and their motivations when presenting the insight gained from interviews in empirical research.

Furthermore, cyber security is a topic where interviewees can understandably be reluctant to discuss sensitive issues candidly. In the research of this thesis, this not only related to matters of national security, but also the often-awkward relationships and dynamics that exist between actors.

[150] William S Harvey, "Strategies for Conducting Elite Interviews," 436.
[151] Glenn Beamer, "Elite Interviews and State Politics Research," State Politics & Policy Quarterly 2, no.1 (2002): 86-96.
[152] Patrick Biernacki and Dan Waldorf, "Snowball Sampling: Problems and Techniques of Chain Referral Sampling," *Methods and Research* 10, no.2 (November 1981): 141-163.

It is therefore important to triangulate the findings with other data sources[153] (both to overcome bias and to research areas where those with expertise are reluctant to be interviewed or discuss issues openly). A range of primary source documents were also examined. This included government strategies, leaked emails, reports, and speeches. These sources were examined with a similar intention to that of the interviews –to establish the incentives, capabilities, and interactions of security actors. Here, these additional data sources provide useful additional insight. For example, the 2016 UK Government cyber security strategy includes claims that the market has failed to appropriately invest in cyber security and argues that further government intervention is required, showing how the UK Government is challenging the role of corporations; Apple CEO Tim Cook's statement on the importance of encryption illustrates how technology firms are actively challenging the stance of US law enforcement agencies; a joint Estonian Government-Microsoft report on their combined data embassy project provides insight into public-private partnerships within Estonia. With so many of these dynamics reflected in the public realm, these additional primary source documents are a vitally important component of the research in this thesis.

Although legal documents are used and cited as primary source data, this thesis does not claim to speak authoritatively on legal and regulatory issues. Crucially, court cases, laws, and regulation are discussed to provide context into assemblages and their dynamics. A more in-depth analysis is out of scope in this thesis, although there would certainly be value in research exploring these issues further and it is hoped that the findings of this thesis could provide relevant context and insight towards such a research project.

For case studies, the most important use of such documentation is to corroborate and augment evidence gained from other sources (such as interviews). It is also possible to make certain

[153] Yin, *Case Study Research: Design and Methods*, 103.

inferences from documents – for example, the distribution list for a specific document, may reveal details regarding security configuration or the role and power of certain security actors.[154]

Finally, this thesis will also draw on a review of secondary or academic literature. Although cyber security is a nascent topic in security studies, areas such as CNI and encryption are fast becoming topics of interest for IR academics. Literature from other disciplines such as risk management and computer science can also provide important insights given that cyber security expertise is distributed across a range of academic disciplines and thought silos.

Related to the data collection, a number of limitations should be recognised. Details in the cyber domain are often poorly understood. Given the sensitivities of the topics at hand, it can be difficult to arrange interviews or to get participants to speak openly about issues of cyber security – a challenge noted by other academics researching similar topics.[155] This is most clearly the case in the context of critical national infrastructure. Many high-profile hacks and attacks are accompanied by a number of potential theories of an aggressor's identity and motivations. Likewise, with many states operating via private actors in order to claim plausible deniability, the relationship between these groups and state institutions are often, by design, difficult to establish. Even the details of more publicly visible relationships, such as corporate public-private partnerships, can be difficult to access, with contract terms often prohibiting the disclosure of relevant details.

Various challenges therefore exist in regard to accessing information, with a number of actors and individuals likely to be unwilling to discuss or be observed given the sensitivities in what they do. This is reflected in access to interviewees and the extent to which they will be willing

[154] ibid., 103.
[155] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies," 46; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," 10

to talk openly. By extension, sensitive topics are less likely to have accessible documentation and secondary literature. Access limitations to certain actors or facts within a case study inevitably mean that the findings of this thesis may be distorted to some degree. Throughout the case studies, issues of access will be discussed. Any potential biases due to a lack of access to certain groups will be openly acknowledged. Some of these limitations are at least partly mitigated given the focus of this thesis on defence and the provision of security – as opposed to more offensive measures and strategies that are naturally even more covert. For offensive actions, actors will usually try to obfuscate their identity, often by acting via a state proxy[156] or by using a front (such as through a pseudonym that claims to be a non-state actor).[157] By contrast, defensive provision is markedly less controversial or covert. The US encryption debate includes numerous public statements by public and private actors alike that can be analysed for example. Although aspects of CNI protection are still highly confidential, this tends to be in relation to details about specific systems and processes. The configuration of security actors, on the other hand, is a less sensitive detail – and one that makes further study possible.

Chapter Summaries

Chapter Two addresses many of the concerns identified in this chapter related to assemblage literature and develops a theoretical model that makes it possible to consider the security implications that arise from thinking with assemblages. It is this theoretical model that provides a conceptual framework used in the following empirical case study chapters.

[156] Jamie Collier, "Proxy Actors in the Cyber Domain: Implications for State Strategy," *St Antony's International Review* 13, no. 1 (2017): 25–47.
[157] Sam Thielman and Spencer Ackerman, "Cozy Bear and Fancy Bear: Did Russians Hack Democratic Party and if So, Why?," *The Guardian*, June 29, 2016, https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc.

Chapter Three will explore encryption in the US. The issue of encryption is of increasing importance to IR with the process of encoding messages enabling individuals to communicate anonymously with one another and without their communication being intercepted. The process of encryption has begun to feature prominently within larger debates related to the appropriate balance between security and privacy in the context of counter-terrorism and intelligence gathering. The issue also reveals fissures between governments and private actors. Technology firms have made encrypting their user's devices and communication their first priority. Encryption is an especially pertinent issue where tyrannical regimes rule; here, encryption provides a means for communication amongst dissidents and can even play a role in facilitating protest and civilian action movements. The US has seen these issues as an important matter of foreign policy and has funded initiatives such as Tor, an internet browser that anonymises dissidents and enables them to access the internet and communicate securely. At the same time however, the software is being used to set up online markets that sell illicit drugs, weapons, and hacking tools that undermine governments. The assemblage studied is therefore characterised by tension and disharmony. Two diametrically opposed visions of security clash. Technology firms and law enforcement entities both vie for power.

Chapter Four will examine CNI in the context of the UK. The protection of critical infrastructure has long been of interest to security scholars and policymakers. A number of industries such as power grids, healthcare services and transport networks have turned to digital technologies to deliver efficiency and cost savings. Yet, a significant proportion of CNI is reliant on embedded hardware and (often proprietary) protocols that predate the Internet. This leaves portions of CNI potentially vulnerable and exposed. Examining the assemblage that protects these assets in the UK, it is argued that a variety of incentive structures exist within the assemblage that has caused inefficient security outputs. Moreover, government actors are increasingly questioning, and even challenging the role of private corporations. Yet, despite

current public tensions, government entities are limited in the scope to which they can actively change current security provision. This means that many of the ongoing security challenges and deficiencies of the current CNI cyber security assemblage are likely to sustain going forward.

Chapter Five will look towards the security provision of Estonia's digital society. Since regaining independence in 1991, Estonia has looked to technology as a key pillar in overcoming the legacy of the Soviet Union.[158] Today, the country is one of the most connected in the world.[159] Alongside the benefits of this approach, there are risks. As the use of technology increases, so too does the country's reliance. With technology at the core of a variety of functions, there are a variety of attack vectors. Furthermore, Estonia's sits at a precarious geopolitical position given its proximity to its neighbour in Russia – a country that has previously targeted the small state. Securing this concept of digital society is therefore vital and as this chapter will show, an issue taken seriously across the country with active participation in security provision across a range of security actors. In this regard, the Estonia digital society assemblage is the most harmonious and stable of the three case studies, showing how various security actors can come together in a positive and cooperative manner, albeit under specific conditions that are largely limited to small states.

Finally, Chapter Six will summarise the empirical findings and discuss their implications for IR theory and future research in cyber security. The implications of using assemblages – a concept that contains its fair share of theoretical and ideological baggage – will also be discussed. The conclusion will also reflect on the central research question and examine the

[158] "How Did Estonia Become a Leader in Technology?" *The Economist*, July 30, 2013, https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology.
[159] Tim Mansel, "How Estonia Became E-Stonia," *BBC News*, May 16, 2013, http://www.bbc.co.uk/news/business-22317297.

notion of the territorial state more broadly in relation to contemporary cyber security challenges. The conclusion will also consider whether the empirical findings have any wider implications on existing IR literature and critical theory. Specifically, it will be argued that IR and security studies should further acknowledge the benefits of an assemblage approach and further integrate issues of security provision into the discipline. Finally, on the basis of these findings, the chapter will identify further research avenues.

Chapter Two: Cyber Security Assemblage Theory Building

Theoretical Model

This chapter presents a theoretical model that further develops assemblage thinking. Chapter One established that an assemblage approach provides a coherent and useful metaphor for understanding contemporary security provision – especially in cyber security contexts given the typically diffuse nature of security structures. Assemblage literature therefore deserves credit for bringing a rich conceptual depth and thick description to understanding nascent security practices. Despite this useful contribution, however, previous assemblage literature has at times fallen short with the opportunity to fully explore the dynamics and implications of diffuse security structures often missed. Research that is descriptively rich, yet lacking in discussion of consequences and implications, ultimately leave key portions of the assemblage literature running hollow – an imbalance the model in this chapter seeks to correct.

This chapter outlines a theoretical model that provides a conceptual framework that anchors the following empirical case studies. It offers a means to reorient assemblage thinking in order to explore soft causal elements – both in relation to how cyber security assemblages have come to be, as well as how the dynamics of an assemblage affect security outcomes. Many of the aspects of this model have been observed before (both in assemblage and cyber security literature). The contribution here is therefore in developing a framework that provides a more structured and schematised way to approach such questions and to redress the descriptive focus of current assemblage thinking. This is not to say that such thick description is not useful in

itself – just that the useful insights that could be derived from exploring further remain untapped.

Each concept within the theoretical model will be discussed in turn below, providing a schematised approach to the following empirical case study chapters. The model also establishes various criteria to capture the internal processes that exist within assemblages – thereby providing comparison between case studies. By showing how the assemblage concept can be mobilised to further explore the implications of contemporary security provision, it is hoped that the model will represent a standalone theoretical contribution to IR, even if readers disagree with aspects of the cyber security and empirical arguments made.

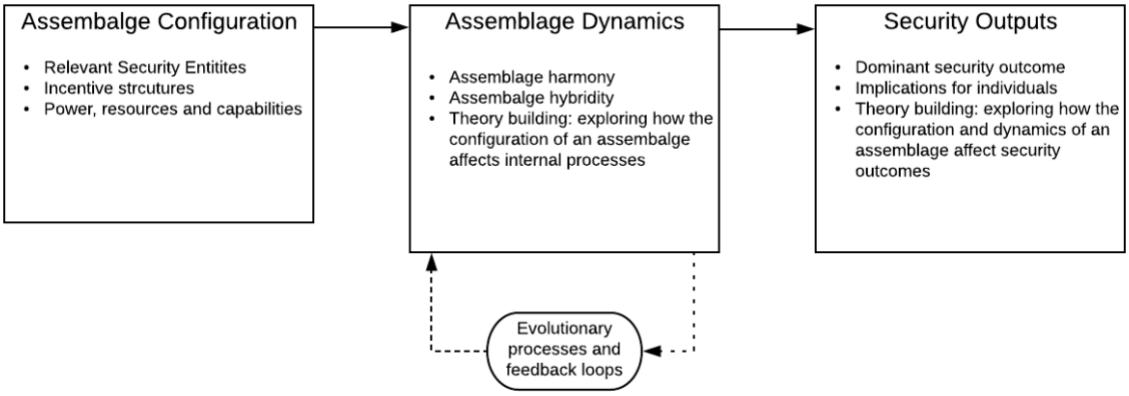

Figure One: Assemblage theoretical model

As seen in Figure One, the Assemblage Theoretical Model comprises three parts: Assemblage Configuration, Assemblage Dynamics, and Security Outputs. The first of these, Assemblage Configuration, is very much in line with traditional assemblage literature that largely seeks to

understand the boundaries of an assemblage and the entities that reside within it. Assemblage Dynamics builds on this initial understanding to explore the internal dynamics within an assemblage, exploring aspects such as fusion, harmony, and the stability of cyber security structures. Finally, Security Outputs questions how the configuration and dynamics of an assemblage have a bearing on the nature of security provision for individuals. Each of these three parts require further elaboration and are discussed in turn below. The chapter then concludes with an outline of how the model is applied to the following empirical case study chapters.

Assemblage Configuration

The Assemblage Configuration is the first component of the theoretical model and provides a means for capturing the essential makeup of assemblages through discussion of relevant security entities and their essential attributes. As well as providing a useful mapping exercise, the concepts that feed into the Assemblage Configuration also enable different assemblages to be compared. It is this section of the model that is perhaps most similar to actor network theory approaches that seek to make sense of diffuse social structures.

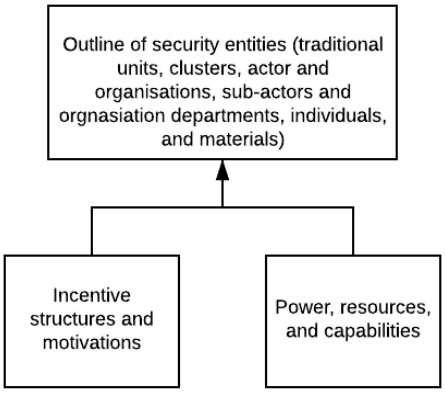

Figure Two: Assemblage Configuration

An outline of relevant security entities forms the central component of the Assemblage Configuration. Security entities can be classified through six tiers with more or less segmented language depending on the level of detail required. The majority of this thesis is focused on the first three however.

The first tier, traditional units, represents the broadest and most overarching groups that have been used traditionally in security studies and IR. This includes corporations (or the 'private sector'); governments; international organisations and networks; civilian groups; academia; knowledge, advocacy, and pressure groups; and media and news outlets. Assemblage thinking typically seeks to move beyond these terms on ontological grounds – both in order to afford a greater agency towards the specific entities that sit within such units and to account for hybrid structures that intersect such traditional distinctions altogether. This thesis, therefore, focuses predominantly on specific actors, rather than overarching categories. Yet the application of traditional units is not completely obsolete despite their rigidity. The benefit of having such broad groups is that they can be applied universally, used throughout all three of the case studies

in order to organise the initial outline of security actors. It is also possible to explore the extent to which these units remain coherent, especially when the variety of actors that sit within them are then examined more specifically. Therefore, while these traditional categories are certainly rigid, they are by no means irrelevant. Unfortunately, the debate over these terms in security studies and IR is often too binary– they are either staunchly retained (as is often the case in realist literature) or outright rejected (as seen in much of the critical literature that embraces postmodernism). This thesis instead seeks to embrace a happy middle path – using such traditional units as an initial organising device, before building in further differentiation and nuance through the additional classification tiers below.

The second classification tier, clusters, provides a means for correcting the often overly blunt conceptual instruments of traditional IR units. Assemblage clusters can either be used to capture groups of actors that reside within a traditional unit (an intra-unit cluster) or those that transcend such distinctions altogether (an inter-unit cluster). The cluster tier is therefore as much a tool used to reformulate actors and assemblages beyond traditional units as it is its own standalone classification tier. Traditional units often comprise a range of different entities that might benefit from being packaged together. In the US case study for example, it is helpful to cluster profit-motivated and non-profit motivated corporations that advocate strong-encryption independently (given the tensions and differences between the two groups). Likewise, creating an intra-unit cluster for all the intelligence agencies that sit within the US Government also provides a useful framing for examining a specific community of government entities. These clusters that sit within traditional units articulate the spectrum of categories and motivations that exist within a single traditional unit.

Inter-unit clusters then provide an additional thinking tool for exploring coherent groups of actors that share a similar set of incentives that exist within a variety of traditional units. A

mixture of government entities, corporations, civil society groups and media outlets are all united (often informally) in their support for strong-encryption in the US for example. A public-private partnership represents the prevailing cluster in the UK CNI Assemblage. Reformulating through inter-unit clusters naturally therefore captures hybrid entities – either in reference to the assemblages as a whole or specific camps of actors within them. The cluster classification tier therefore provides an initial foundation for exploring assemblage hybridity (a concept then developed further in the following Assemblage Dynamics section of the model).

The third classification tier, actors, then turns to specific organisations themselves. This might include specific government entities such as the UK Cabinet Office or the Estonian Ministry of Economic Affairs. Individual firms such as Apple, Facebook and Google also sit in this category. Even when groups of actors can be clustered together, there are often further differences and tensions between them, making it important to examine individual actors in isolation. The US law enforcement and intelligence community would be one example of a group that is on the one hand a coherent intra-unit cluster, yet nonetheless there remains clear tensions and divergences between agencies given their different incentive structures (with it therefore making sense to explore these organisations both as a group and on their own). Inevitably an interpretative judgement call is made in determining what constitutes a relevant security actor with the intention being to identify the key entities involved in providing security and determining the makeup of Assemblage Dynamics. Examining organisations specifically makes it possible to understand these dynamics and relationships in further depth.

The spirit of assemblage thinking naturally involves going beyond the traditional units used in IR. It is a tool that makes deep segmentation beyond 'the state' or 'the private sector' possible. The level of demarcation applied here is comparatively modest when compared to the full possibilities of assemblage thinking, given the broad focus on actors and how they cluster

together. Other assemblage thinkers have gone much further. Michele Acuto and Simon Curtis, for instance, have argued that the concept is capable of accommodating 'the various hybrids of material, biological, social and technological components that populate our world.'[160] Categorising an assemblage through a focus on organisations might, therefore, be seen as against the spirit of an approach that moves away from the 'anthropocentrism that characterizes the vast majority of historical and political writing.'[161] Yet, any segmentation ultimately involves trade-offs. Unpacking further certainly provides additional details, yet also risks introducing excessive complexity. At some point, further segmentation only offers nuance for its own sake, restricted largely to self-referential academic debates. The three classification tiers discussed above are all vital for this thesis – the additional insights gained from each tier brings unique insights and clear added value that is highly relevant to the central research question. While a judgement was made that digging deeper would not materially aid the analysis, a further three possible tiers (sub-actors, individuals and materials), are outlined briefly below in order to provide a complete theoretical model. These additional tiers might be more relevant to other assemblage studies (and two of which are used occasionally in passing within this thesis).

The forth tier of the theoretical model is sub-actors or organisational departments (such as the Engineering and Technology team at Google or the Office of Cyber Security and Information Assurance that sits within the UK Cabinet Office). A university (which would be categorised as an actor in the third classification tier) might be more coherently divided via academic departments (classified as sub-actors) for instance. Likewise, a cyber security team will naturally prioritise security while business and marketing teams might be more focused on

[160] Michele Acuto and Simon Curtis, "Assemblage Thinking and International Relations," 2.
[161] ibid., 2.

getting products and services to the market quickly and with exciting features, even if they pose security risks.[162]

Segmenting further, the fifth tier turns to individuals. This could involve either a focus on specific individuals that have had a significant influence on security provision (the US case study discusses Edward Snowden as a standalone individual for instance). It might also involve examining employees, who often have the agency and capability to impact their organisation in ways that materially affect security provision. Employee discord at Google was a major factor in the organisation deciding to abandon certain agreements to work with the US Government on the military application of artificial intelligence for example.[163]

The final tier involves material objects – the analysis and incorporation into security structures of which has become increasingly popular in IR through the so called 'material turn' that has been adopted enthusiastically by assemblage thinkers.[164] Digital technology, malware and autonomous software are becoming an increasingly important part of security structures for example. Although this is not in scope for this given time and resource constraints, it is an avenue of enquiry that contains exciting research possibilities.

[162] Jamie Collier and Andrew Martin "Beyond Awareness: the Breadth and Depth of the Cyber Skills Needed" *Cyber Studies Working Paper* (Forthcoming).
[163] Kate Conger, "Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program," Gizmodo, June 1, 2018, https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620.
[164] Antoine Bousquet, "Welcome to the Machine: Rethinking Technology and Society through Assemblage Theory," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis (London, UK: Palgrave Macmillan UK, 2014), 91–97; Roger Mac Ginty, "A Material Turn in International Relations: The 4x4, Intervention and Resistance," *Review of International Studies* 43, no. 5 (December 2017): 855–874; Diana Coole and Samantha Frost, eds., *New Materialisms: Ontology, Agency and Politics* (Durham, UK: Duke University Press, 2010); Tom Lundborg and Nick Vaughan-Williams, "New Materialisms, Discourse Analysis, and International Relations: A Radical Intertextual Approach," *Review of International Studies* 41, no. 1 (2015): 3–25.

Classification Tier	Description	Examples
Sectors	Broad and overarching sectors comprising different actor groups.	Governments, the private sector, international and transnational networks
Clusters	Blocs of actors and organisations within and between sectors, classified through a coherent theme or issue-area. Used to segment traditional units and to build groups of actors that transcend traditional units.	Pro-encryption advocates, multinational firms, civil society coalitions.
Units	Specific actors and organisations	Apple, New York Times, National Grid, Estonian Defence League's Cyber Unit.
Sub-units	A specific team or divisions that exist within an organisation.	Microsoft’s Global Security Strategy and Diplomacy Team, National

		Security Agency Tailored Access Operation unit
Individuals	Either a standalone security entity or an employee / member of a security actor.	Edward Snowden, FBI employee
Materials	Non-human material objects	Stuxnet code, AI algorithms

Table One: Classification Tier Schema

When discussing relevant security entities, two essential attributes feed into the Assemblage Configuration analysis: incentive structures and power. Incentive structures relate to what drives each security entity with two aspects considered. First, the incentives that motivate an entity – for example, whether they are financially driven, seek to grow and develop, hope to improve their reputation, etc. Second, the desired outcomes of the security actor are also relevant. Even if governments and private sector firms have different motivations, they may share a desired outcome (for example, both political and financial-motivated actors might share the same desire to improve the security of critical national infrastructure). Likewise, two profit-driven private sector firms may hope for altogether different outcomes: a cyber security firm hired to prevent cyber attacks in the first place hopes their clients remain secure while a business that specialises in helping organisations in the immediate aftermath of a serious data breach or cyber crisis situation instead profits from such incidents.

A vast literature on the topic of power exists in IR, with consensus on the meaning of the term difficult to achieve. Hans J Morgenthau claimed that the concept ‘poses one of the most

difficult and controversial problems of political science'[165] while Kenneth Waltz has argued that its 'proper definition remains a matter of controversy.'[166] Robert A Dahl has suggested that despite disagreement over the relevant terms related to power (such as coercion, force and persuasion), most definitions of power come down to a sense of Actor A causing (or having the ability to cause) Actor B to do something that they would not otherwise do.[167] Yet, this notion of power is not necessarily applicable for the purposes of this thesis. Within an assemblage framework, emphasis is placed on how understandings of hierarchy, ranking and influence, as well as the roles of actors are being mutually defined and established.[168] Here, the ability to get other actors to do something is secondary compared to an actor's own ability to establish itself as a relevant and meaningful security provider. Here, Max Weber's notion of power is thus more appropriate, defined as 'the probability that one actor within a social relationships will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests.'[169] Instead of power being defined by shaping the actions of others, Weber's definition focuses instead on an actor's own aims and ambitions. Within an assemblage framework, security actors have a general goal of establishing themselves as relevant and meaningful security providers – power, therefore becomes the means that enable security actors to realise this goal. The term is thus linked to the capability and resources of security actors that help them to achieve this. While linking power with resources has previously been criticised, this has typically been in the context of producing indexes or

[165] Hans J Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, (New York: Alfred A Knopf, 1963) pp. 27.
[166] Kenneth N Waltz, "Reflections on Theory of International Politics: A Response to My Critics," in *Neorealism and its Critics*, ed. Robert O Keohane, (New York: Columbia University Press, 1986), 322–345. pp 333.
[167] Robert A Dahl, "The Concept of Power," *Behavioural Science* 2, no. 3 (July 1957): 201–215.
[168] Rita Abrahamsen and Michael Williams., "Tracing Global Assemblages, Bringing Bourdieu to the Field: A Conversation with Rita Abrhamsen and Michael Williams."
[169] Max Weber, *Economy and Society: An Outline of Interpretive Sociology*, ed. Guenther Roth and Claus Wittich, (Berkeley, CA: University of California Press, 1978). pp. 53; Mark E Warren, "Max Weber's Nietzchean Conception of Power," *History of the Human Sciences* 5, no. 3 (1992): 19–37.

rankings that determine the relative power of states or actors.[170] Here, the intention is different given that the aim is not to quantify the power of various security actors, but instead to understand their various attributes and how this enables them to solidify their position as a security actor.

It is also worth emphasising that the definition of power used in this thesis is distinct from the notion of 'power diffusion' that has previously been discussed within cyber security literature.[171] Power diffusion refers to a process whereby relative power is transferred from dominant actors within the international system to a larger number of non-traditional or non-state actors that have been perceived as comparatively less powerful. The term has typically been used in a cyber security context to capture the way that low barriers to entry have enabled non-state actors to make a significant impact when compared to other more traditional security contexts. While this thesis explores how this broader power diffusion process impacts cyber security provision, the definition of power outlined above is instead focused on the capabilities of security providers themselves. Crucially, if power diffusion processes have occurred in a cyber security context, then the definition of power used in this thesis provides an empirical analysis that captures the capabilities of specific actors. Both the process of power diffusion and an analysis of security actors' powers are discussed in this thesis; while linked, these two concepts are therefore not interchangeable.

The Assemblage Configuration part of the theoretical model not only outlines the relevant actors and their essential attributes, but also provides a means for organising the various

[170] Peter Morriss, *Power: A Philosophical Analysis*, (Manchester, UK: Manchester University Press, 2002); David A Baldwin, "Power and International Relations," in *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse, and Beth A Simmons, (London: Sage, 2007), 273–97. pp. 279.
[171] Joseph S Nye Jr, The Future of Power, 113-152

groupings that exist through various classification tiers. This provides an important foundation that develops the fundamental makeup and boundaries of an assemblage.

Assemblage Dynamics

Assemblage Dynamics moves beyond a mapping of the actors to explore the internal processes that exist within security structures – the extent of cooperation occurring between actors; the power clashes and tensions that occur; where dominance lies; etc. Assemblage Dynamics are explored through three terms: hybridity, harmony and evolution. These three terms both articulate the essential characteristics of an assemblage and provide variables to compare between assemblages. The empirical case study chapters will both discuss these internal processes and identify the possible reasons why such dynamics have come to exist in the first place.

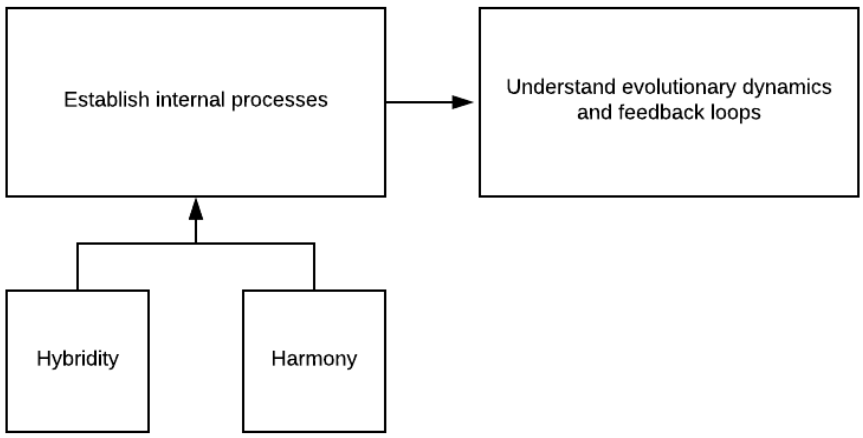

Figure Three: Assemblage Dynamics

Hybridity explores the amalgamation between entities in an assemblage. The concept is used to consider the extent to which ontological distinctions between actors remain coherent and justified. A highly hybrid assemblage is therefore a structure with blurry distinctions and overlapping boundaries. Actors in hybrid structures are less ontologically distinct, and instead more appropriately framed as part of a broader network of similar actors that regularly interact as a collective. Conversely, a highly fragmented structure is one with a variety of far more ontologically distinct entities that clearly operate independently.

The practices that occur within an assemblage are examined in order to establish the fusion of security structures. Practices are defined as socially meaningful patterned actions that are embedded in an assemblage structure, and are articulated through specific types of action.[172] Whilst there is an emerging body of literature in IR focused on practices and practice theory,[173] these ideas are not explored in the same level of depth within this thesis. Instead, the term practice is used simply as a concept to capture actions that occur between actors, with consideration on the extent to which such practices embed actors together or conversely drive them further apart. Information sharing, for example, represents a practice that binds actors together when a single information exchange is used by a variety of actors (who share the same infrastructure, systems, staffing, data, etc).[174] Outsourcing is a practice that could potentially exhibit hybridity, although this is not guaranteed. For instance, outsourcing might not affect fusion if the contractor and the client remain clearly separated. However, if contractors become

[172] Emanuel Adler and Vincent Pouliot, "International Practices," *International Theory* 3, no. 1 (2011): 1–36. pp.5.
[173] Theodore R Schatzki, Karin Knorr Cetina, and Eike von Savigny, eds., *The Practice Turn in Contemporary Theory* (London, UK: Routledge, 2005); Emanuel Adler and Vincent Pouliot, "International Practices," (2011); Emanuel Adler and Vincent Pouliot, *International Practices* (Cambridge, UK: Cambridge University Press, 2011); Rebecca Adler-Nissen, ed., *Bourdieu in International Relations* (Abingdon, UK: Routledge, 2013); Rebecca Adler-Nissen, "Towards a Practice Turn in EU Studies: The Everyday of European Integration," *Journal of Common Market Studies* 54, no. 1 (November 2015): 87–103.
[174] Warwick Ashford, "UK Government Sets up Cyber Security Fusion Cell," Computer Weekly, March 27, 2013, https://www.computerweekly.com/news/2240180207/UK-government-sets-up-cyber-security-fusion-cell; "Cyber Security Information Sharing Partnership (CiSP)," NCSC, March 20, 2018, https://www.ncsc.gov.uk/cisp.

increasingly embedded with their client, the distinctions between the two actors would blur as fusion increases. This might occur, for example, when contractors regularly hire employees directly from their client; when both contractors and their client share the same office space; and when both parties perform similar and overlapping functions.

Practices can also actively fragment and partition the linkages between actors, thereby reducing fusion. Legal challenges, regulation that compels actors to behave in a certain way, and public criticism would all be examples of practices that could reduce hybridity and harmony by driving a wedge between actors.

The concept of hybridity can be applied to an assemblage as a whole, as well as to certain pockets that reside within it. Assemblages are often referred to as hybrid structures, yet this fails to provide an adequate level of nuance and precision. This is because fusion is rarely uniform throughout an assemblage. Instead, certain clusters of actors will typically be more amalgamated than others. Assemblages could conceivably contain both highly hybrid and highly fragmented pockets.

The emphasis on examining divergent case studies naturally means that a spectrum of fusion exists (see Figure Four below) and the differences and variance within the three assemblages studied forms a central part of this thesis' analysis. Encryption disputes between actors in the US Encryption Assemblage has naturally divided and fragmented security actors. Tensions within both intra-unit and inter-unit clusters further compound the distinctions between actors. The UK CNI Assemblage, by contrast, is partially hybrid – all actors theoretically want the same thing, albeit to different extents and for different reasons. The majority of practices, however, bind and embed actors together. Finally, the Estonia Digital Society Assemblage has remarkably high levels of hybridity with the initial distinctions drawn between actors often proving to be arbitrary.

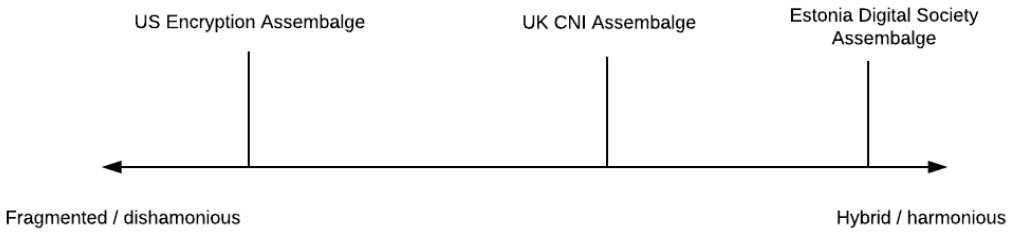

Figure Four: A Spectrum of Hybridity

It is also essential to consider the harmony that exists within an assemblage. This refers to the extent to which converging interests, shared views, and positive (or friendly) relationships exist between security actors. A harmonious assemblage is one where different actors maintain good relationships with each other and share approaches to the referent object being examined. Conversely, a highly tense or disharmonious assemblage is one where actors are regularly challenging each other.

Harmony is also observed through the practices and interactions between security actors. An analysis of contestations, clashing securities and tension between actors and clusters are therefore all essential in determining levels of harmony. The levels of harmony within an assemblage can also be established through interviews by asking participants about how security actors interact and perceive one another.

A central finding of this thesis is that harmony and hybridity often go hand-in-hand. As shown in Figure Four above, the most hybrid assemblage in this thesis is also the most harmonious while the most fragmented assemblage is also the more disharmonious. Yet, the two concepts remain distinct. Hybrid structures naturally require a group of actors to share some level of common interests and desired outcomes. This means harmony is an important component of fusion. Yet, the presence of harmonious clusters, while a necessary precondition, is not on its

own a mark of hybridity. It could be that a group of actors share the same vision of security and maintain positive relationships with one another, yet remain ontologically distinct – all working on the same challenges simultaneously, yet in largely independent capacities. It is therefore possible for a security structure to be harmonious, but not hybrid.

Assemblages are not static structures.[175] The extent of hybridity and harmony, and the practices that occur in an assemblage, are all liable to change.[176] Assemblage dynamics shift as new initiatives emerge and as relationships between actors change over time. Assemblage dynamics will invariably improve if various actors buy into partnership arrangements. Emerging practices might conversely further divide or disrupt dynamics and relationships within clusters. Actors themselves also change. Indeed, it is the notion of assembly and disassembly – where actors relinquish, transfer and develop capacities and functions – that is central to the added value of the assemblage concept.[177] Actors assemble greater capabilities and responsibilities as they grow in stature and capture the remit of cyber security challenges. Technology firms are increasingly wading into profoundly political issues, thereby assembling into more overtly political actors.[178] Conversely, certain cyber security issues are increasingly regulated, legislated, and captured by government entities – thereby disassembling aspects of private actor

[175] Saskia Sassen and Aihwa Ong, "The Carpenter and the Bricoleur: A Conversation with Saskia Sassen and Aihwa Ong."
[176] ibid., pp. 23; Christian Bueger, "Thinking Assemblages Methodologically: Some Rules of Thumb," in *Reassembling International Theory*, ed. Michele Acuto and Simon Curtis (London, UK: Palgrave Macmillan UK, 2014), 58–66. pp. 62.
[177] Jamie Collier, "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision," *Politics and Governance* 6, no. 2 (June 11, 2018): 13–21. pp. 15; Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages*, pp. 21; Rita Abrahamsen and Michael C Williams, *Security Beyond the State: Private Security in International Politics* (Cambridge, UK: Cambridge University Press, 2011); Rita Abrahamsen and Michael C. Williams, "Security Beyond the State: Global Security Assemblages in International Politics," *International Political Sociology* 3, no. 1 (March 2009): 1–17.
[178] For example, social media platforms are increasingly establishing moderation policies with clear political and philosophical dimensions - the line between hate speech and free speech for example. Likewise, private cyber threat intelligence firms are developing policies on when to attribute the cyber activities of state groups. See, Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (New Haven, CT: Yale University Press, 2018); Zaid Shoorbajee, "Playing Nice? FireEye CEO Says U.S. Malware Is More Restrained than Adversaries," Cyberscoop, June 1, 2018, https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice/.

agency while enhancing the standing of government entities and international organisations. New actors may emerge in an assemblage, quickly establishing themselves as influential[179] while established actors and institutions have previously diminished in stature.[180] Contemporary cyber security practices are replete with these instances of assembly and disassembly. Assemblage thinking therefore pays attention to how shifts in the capabilities and roles of actors affect security structures.

Assemblage dynamics are also contingent on events. Russian cyber-attacks on various Estonian systems in 2007 mobilised the Estonian Digital Society Assemblage;[181] the domestic backlash of Edward Snowden leaking sensitive NSA documents led to fundamental shifts with technology firms distancing themselves from the US Government by introducing robust encryption measures;[182] the UK's commitment to leave the European Union will inevitably affect the role that the international organisation will play in future UK cyber security and intelligence sharing issues.[183]

[179] For example, encrypted messaging applications Telegram and Signal were founded in 2013 and 2014 respectively and have gone on to be important stakeholders in contemporary US encryption disputes.
[180] The cyber norm building programme at the United Nations being one obvious example. See, Alex Grigsby, "The End of Cyber Norms," *Survival* 59, no.6 (November 2017): 109–122; Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" The Diplomat, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.
[181] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security" (10th European Conference on Information Warfare and Security 2011, NATO CCDCOE, 2011); Camille Marie Jackson, "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success," New Voices in Public Policy 7 (2013); Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, https://www.bbc.co.uk/news/39655415.
[182] Christopher Soghoian, "Snowden's Leaks Have Finally Forced Companies to Enhance Their Security," MIT Technology Review, December 17, 2013, https://www.technologyreview.com/s/522756/snowdens-leaks-have-finally-forced-companies-to-enhance-their-security/; Hannah Kuchler, "Tech Companies Step Up Encryption in Wake of Snowden," Financial Times, November 4, 2014, https://www.ft.com/content/3c1553a6-6429-11e4-bac8-00144feabdc0; Trevor Timm, "Four Ways Edward Snowden Changed the World – and Why the Fight's Not over," The Guardian, June 5, 2014, http://www.theguardian.com/commentisfree/2014/jun/05/what-snowden-revealed-changed-nsa-reform.
[183] Shavana Musa, "Data Protection, Intelligence-Sharing and Brexit: The Path Ahead," August 2, 2017; Kat Hall, "Security Execs Must Prep for Post-Brexit Cyber Challenges," The Register, June 11, 2018, https://www.theregister.co.uk/2018/06/11/cisos_must_be_braced_for_cyber_security_challenges_post_brexit_report/.

The shifting dynamics and changing nature of cyber security structures means it is important to consider how assemblages are continuously evolving and how actors and clusters react to one another through feedback loops. Recent encryption disputes provide a case in point: the US District Court for the Central District of California initially sought to compel Apple to assist the FBI in unlocking an iPhone through a court order;[184] Apple then refused, responding with public statements stressing the importance of privacy and security;[185] the FBI subsequently purchased exploits from contractors to break into iPhones without Apple's assistance;[186] Apple then updated user software to make it harder for law enforcement to gain access to phones;[187] etc. These osculating dynamics are observed in a variety of security settings with a single action often going on to producing an entire chain of events. Discussing shifts over time help to contextualise the current situation, as well as make some suggestions for how such internal processes may develop further going forward.

Studying the evolution of an assemblage also accounts for the agency of security actors and individuals themselves. While this thesis is primarily focused on how variables including harmony and hybridity affect security outputs, security actors also affect security outputs independently. This idea is already integrated into the framework by studying actors incentive structures (which represent at least an aspect of an actor's agency). Yet, a study of evolution allows for a more in depth examination of agency by exploring how actors interpret and react

[184] Eileen M Decker et al., In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (United States District Court for the Central District of California February 16, 2016).
[185] Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, http://www.apple.com/customer-letter/.
[186] Mark Hosenball, "FBI Paid under $1 Million to Unlock San Bernardino iPhone," Reuters, May 4, 2016, https://uk.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUKKCN0XQ032; Alina Selyukh, "The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?," NPR.org, February 23, 2016, https://www.npr.org/sections/alltechconsidered/2016/03/23/470573608/the-apple-fbi-whodunit-whos-helping-the-feds-crack-the-locked-iphone.
[187] Jon Brodkin, "FBI Security Expert: Apple Are 'Jerks' About Unlocking Encrypted Phones," Ars Technica, January 11, 2018, https://arstechnica.com/tech-policy/2018/01/fbi-security-expert-apple-are-jerks-about-unlocking-encrypted-phones/.

to an assemblage's configuration, dynamics, and security outputs, as well as how their reactions impact these variables over time.

Studying these internal processes develop the assemblage analysis further. Approaches that simply deconstruct or critique state-centric paradigms are often unsatisfactory when they do not then seek to explore what this means or propose alternative conceptual models. Up to this point, however, the focus has been entirely on the security providers that sit within an assemblage.

Security Outputs

The final part of the theoretical model expands to address the significance of the configuration and dynamics of an assemblage through a consideration of broader security outputs.

Security outputs examine the overall security outcome of the referent object being studied (i.e. the data security of American citizens, the security of UK CNI, or the integrity of Estonia's digital society infrastructure). In doing so, this thesis determines the impact that the variables previously discussed (including an assemblage's configuration, the distribution of power, the incentive structures of security actors; and an assemblage's levels of harmony and hybridity) have on security. A central argument of this thesis is that an assemblage theoretical approach provides new insight when compared to traditional IR approaches focused on power and interests. A discussion of security outputs achieves this by highlighting how the issues that are central to an assemblage approach are vital for understanding security.

Assemblage processes clearly have a bearing on the nature of cyber security provision, yet connecting these variables to actual consequences remains underexplored. Investigating this relationship is useful for two reasons. First, it provides a form of theory building. Although formal causal theory testing is avoided, this thesis still seeks to offer insights by at least

beginning to develop and identify possible hypotheses that might further clarify how the dynamics of security structures affect security outcomes. This is achieved by identifying various concepts and variables (including hybridity, clusters, harmony, and evolution) and considering their impact on security. If the majority of actors enjoy positive relationships with each other, share a uniform vision of security, and become increasingly amalgamated with one another, there is a high chance that this will lead to a relatively stable and uniform notion of what form of security is provided. By contrast, a fragmented assemblage fraught with tension and power distributed across a range of actors with different incentive structures will lead to a less stable security outcome that is contingent on the disputes and interactions between security actors.

In discussing security outputs, it is useful to establish if the variables examined in this thesis produce a good and healthy security outcome or not. This means it is necessary to establish what a positive or negative security outcome would look like. At its core, a positive security outcome is one where the referent object under examination is secure (i.e. is suitably defended against potential attacks).

Yet, establishing a security outcome is more complicated than just establishing if a referent object is suitably defended. This is because multiple securities exist for many referent objects. An objective view on what 'good' security means is contested. While the security of CNI is largely straightforward (i.e. CNI that is not compromised), data security is a far more problematic issue. Here, some would argue that a positive security outcome would be data that is encrypted in a way where no one apart from a sender and recipient can access it. Yet, it could be argued that such a security outcome is fundamentally insecure, given that encrypted data can allows terrorists, child exploitation, and organised criminals to flourish. This highlights

both the contested nature of cyber security, as well as the way these issues impact other areas of national security.

When an objective view on what constitutes a positive security outcome is not possible to establish, it is necessary to consider the democratic embeddedness of security. This means the extent to which the security outcome reflects the democratically-held views of the individuals that reside within an assemblage. While a referent security object could hold multiple and even contested securities, if 95 percent of the individuals within an assemblage favour a particular version of security outcome, then this would legitimately constitute a positive security outcome. By contrast, if the democratic view on a referent object was more disputed, then a positive security outcome would seek to balance the views and preferences of different sides. As discussed in Chapter One, coverage on the securitisation and militarisation of cyber security;[188] the underrepresentation of civil society stakeholders and the oversized role of certain regions and entities;[189] and the incentive gaps that exists between security providers and the public[190] are all trends previously observed and ones that feed into the analysis. Whilst many of these trends have been examined in isolation (a highly useful exercise in itself), it is hoped that this theoretical model provides a means for capturing a number of these trends and processes into a more systematic and cohesive framework. Further exploring these links is particularly important given the skewed coverage of cyber insecurity within IR literature that has placed too much emphasis on the structural factors of the domain and the proliferation of

[188] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School,"; Katarina Klingova, "Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia" (Department of Political Science, Central European University, 2013); Matijn Paalman, "The Copenhagen School in the Fifth Domain: Successfully Securitizing Cyberspace?" (Department of Peace and Conflict Research, Uppsala University, 2013); Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension,"; Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better."
[189] Ronald J Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace,"; Madeline Carr, "Power Plays in Global Internet Governance."
[190] Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies."

threat actors. This thesis seeks to build upon the effective third camp that focuses more on security providers and security practices themselves.

The second reason for examining assemblage security outputs is to establish the impact assemblage configuration and dynamics have on individuals. The previous sections of the theoretical model have focused exclusively on security providers, yet these issues also affect individuals – it is their security which is at stake and which is negotiated and defined within assemblages. Despite the multitude of actors often involved in the provision of cyber security, civil society constituencies are often chronically underrepresented.[191] Crucially, the interests of government entities or private sector firms do not necessarily reflect what is of importance to individuals. There are elements of theatre within cyber security assemblages as various stakeholders appropriate the security and interests of individuals. Technology firms, for example, might claim they are introducing encryption for the purposes of protecting user privacy while simultaneously undermining sensitive user information for the purposes of advertising.[192] Likewise, government agencies might invoke concerns over highly emotive topics such as child exploitation as a means to securitise and capture cyber security issues.[193] All three parts of the theoretical model provide useful and interesting academic insights, yet it is ultimately the implications that they have for individuals that is arguably most important. It therefore represents a fitting area of focus to conclude an approach that is thinking with assemblages.

[191] Madeline Carr, "Power Plays in Global Internet Governance."
[192] Tomas Chamorro-Premuzic and Nathalie Nahai, "Why We're So Hypocritical About Online Privacy," Harvard Business Review, May 1, 2017, https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy; John Naughton, "Google, Not GCHQ, Is the Truly Chilling Spy Network."
[193] James Comey, "Expectations of Privacy: Balancing Liberty, Security, and Public Safety" (April 6, 2016), https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety.

Applying the Theoretical Model to the Case Studies

This chapter has proposed a conceptual model that ties the notion of assemblages and their dynamics to security outputs. Although it should be emphasised that there is nothing inherently wrong with highly descriptive research in IR, previous assemblage research has untapped potential to explore further by uncovering the dynamics and implications of diffuse security structures. The framework discussed above enables assemblage thinking to explore soft causal elements related to both how security assemblages have formed, and how their dynamics affect security provision.

The remainder of this chapter will first outline how the conceptual framework is applied to the case studies. Before an assemblage is outlined and explored in each case study, the chapter introduction section will first provide an overview of relevant terms, set the boundaries of the case (such as the time period studied), and discuss the importance of the cyber security topic in question to security studies and IR more broadly. As noted in Chapter One, cyber security remains a nascent topic in the discipline and so it is appropriate to justify why the various topics (CNI, encryption and digital society) matter – or more crucially, why security studies should 'widen' to accommodate these emergent issues.

The Assemblage Configuration section then represents a mapping and categorisation exercise that will provide an overview of all the relevant security actors within the assemblage and their essentially attributes (i.e. their incentives structures and power). Security actors will be organised by their traditional unit, and then further grouped into intra-unit and intra-unit clusters (where they exist). A discussion of both intra-unit and inter-unit clusters will thereby reformulate the configuration of actors, presenting the most coherent prism or prisms in which to study the assemblage.

Having reformulated actors via clusters, the Assemblage Dynamic section will then explore the internal processes and how they have evolved over time. Assemblage Dynamics will explore endogenous developments – seeking to understand the reasons why an assemblage appears as it does and the relevant factors that underpin such an outcome. This section will be structured via the reformulated clusters established in the previous section, thereby enabling the study to focus on the most coherent prisms for approaching the case study. Various more bounded case examples are then outlined that are illustrative of the broader assemblage dynamics.

Finally, the Security Output section will explain what impact the internal processes and broader assemblage dynamics have on individuals. The discussion will also suggest the exogenous variables (out of those discussed in the Assemblage Dynamics section) are the most significant or influential for the purposes of affecting security outputs.

Chapter Three: The US Encryption Security Assemblage

Introduction

Encryption has proved a highly disruptive influence on US politics. Deep tension and disharmony characterise the US Encryption Security Assemblage. Multiple, yet mutually exclusive, stances on encryption and data security exist – leading to clashing securities. The assemblage is also highly fragmented with the various security actors largely working interpedently. These assemblage dynamics, combined with a dispersed distribution of power, means that individuals are left with an unstable notion of security with the state of encryption and data security in regular flux.

The findings of this chapter provide useful insight into the central research question of this thesis: the assemblage of relevant encryption security actors and the dynamics that exist within this structure have significant implications for the state of encryption security in the US. While the numerous security actors involved have differing and clashing incentives related to encryption, none of these actors have the capability and resources to sustain their security ambitions. This means that encryption security is iterative, constantly shifting as the advantage goes back-and-forth between strong and weak-encryption actors. The security of encryption on a US citizen's devices is therefore constantly changing.

This chapter explores the encryption landscape in the US between June 2013 and February 2018 with the assemblage comprised of the key actors involved in domestic encryption disputes. The focus is therefore specifically on the encryption of user data within the US itself. International actors are discussed (and fall within the US Encryption Security Assemblage)

provided that they have had a decisive impact on US the encryption outcomes of American citizens.

Encryption in the United States: A Contextual History

Before addressing this thesis' central research question in the context of the US Encryption Security Assemblage, it is first necessary to provide relevant definitions, historical context, and outline encryption's importance to IR and security studies.

Encryption provides a method of securing communication and data shared between two parties. A cryptographic algorithm is a mathematical function that converts data that can be read and understood without any special measures (known as plaintext or cleartext) into an unrecognisable, or 'encrypted' form known as ciphertext.[194] Encrypted data is therefore nonsensical when intercepted by a malicious actor or if received by an unintended recipient. An intended recipient that possess an accompanying decryption key, however, will be able to decrypt and understand such data. Encryption has become a fundamental pillar of cyber security and now protects far more than just text – photos, audio files and entire databases are now routinely encrypted. An important distinction exists between on-device and end-to-end encryption. End-to-end encryption, refers to the encryption of data while in transit – for example, messages and video feeds that are sent across networks.[195] Here, data is encrypted between end nodes, keeping it secure in the event it is intercepted by a malicious actor (known

[194] Keith M Martin, *Everyday Cryptography: Fundamental Principles and Applications* (New York: Oxford University Press, 2012); "Introduction to Cryptography." GPGTools, April 13, 2017, https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography.

[195] Howard M Zeidler, End-to-End Encryption System and Method of Operation, 4,578,530 (SanMateo, CA, issued March 25, 1986), https://patentimages.storage.googleapis.com/a7/3b/16/eb638400c54c83/US4578530.pdf; Whitfield Diffie and Martin Hellman, "New directions in cryptography," *IEEE transactions on Information Theory* 22, no. 6 (November 1976): 644-654; Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat Histroy: Lessons from the Crypto Wars of the 1990s" (Washington, DC: Open Technology Institute, New America, June 2015). pp. 2-4.

as a man-in-the-middle attack).[196] On-device encryption refers to the encryption of hardware and devices (including phone, laptops, and remote data centres) and by extension, the data that is stored on these devices (also known as data-at-rest).[197] On-device encryption ensures that data is kept safe, even if a device is stolen or obtained by someone other than the user.

Obfuscating messages has a rich historical tradition. Hebrew scribes wrote down the book of Jeremiah using a reversed-alphabet subsection known as ATBASH in 500-600 BC; the Greeks used a device called the Scytale where a long strip of leather was wrapped and written on, ensuring only those with a staff of the same width could understand the message in 500 BC; Julius Caesar used an alphabet substitution where letters with shifted up or down the alphabet to protect official communications in 100-44 BC.[198]

Since the development of modern encryption systems in the 1970s, the issue has represented an ongoing source of tension between public and private actors in the United States that came to be known as the 'Crypto Wars.'[199] In the Cold War era, US government actors tried to control and prevent the diffusion of sensitive technologies, including encryption technologies, through export control laws. With cryptographic tools having been used almost exclusively by military and intelligence agencies at the time, encryption technologies were even classified as munitions.[200] The NSA later introduced the Clipper Chip in 1993 – a piece of phone hardware that would enable communication to be encrypted while also providing an additional key that

[196] "What is a Man-in-the-middle Attack?," Norton, accessed September 1, 2018, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
[197] Matthew Pettitt, "Encryption at Rest: Not the Panacea to Data Protection" (Manchester, UK: NCC Group Whitepaper, 2017). pp. 3-8.
[198] Keith M Martin, *Everyday Cryptography: Fundamental Principles and Applications*, 48; Mohd Zaid and Waqiyuddin Mohd Zulkifli, "Evolution of Cryptography" 2007;.
[199] Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat Histroy: Lessons from the Crypto Wars of the 1990s,"; Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 7–38.
[200] Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s."

would enable US intelligence agencies to listen in with a court-approved wiretap.[201] These measures were eventually abandoned with US government actors recognising the vulnerabilities inherent in such approaches and accepting the necessity of encryption in a variety of business functions (including the protection of intellectual property and authentication of websites).[202]

After a period of relative stability during the 2000s, well established encryption debates resurfaced in June 2013 when NSA contractor Edward Snowden leaked extensive operational details about the NSA and its partners' intelligence gathering programmes (the leaked documents will hereinafter be referred to as the 'Snowden documents'). Labelled as the beginning of the 'Crypto Wars 2,'[203] the Snowden documents led to significant fallout and tension between different encryption actors in the US. Technology firms sought to distance themselves from the US Government intelligence community and these tensions came to a fore in late 2015 and throughout 2016 after Apple refused to assist the FBI in unlocking the iPhone of, Syed Rizwan Farook's iPhone, a shooter involved in an attack in San Bernardino in December 2015. It is these events that forms the basis of this case study's analysis.

Encryption's importance to IR and security studies is incontrovertible. Encryption, and the ability to break encryption was a crucial factor in the outcome of World War II – it has been suggested that the breakthroughs at Bletchley Park (where the Nazi enigma code was broken) shortened the war between two and four years and could have saved between 14 and 28 million

[201] Stephen Levy, "Battle of the Clipper Chip," New York Times Magazine, 1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.
[202] Interview with a cyber security, privacy, and encryption academic by the author. Skype. April 11, 2018.
[203] Sascha D. Meinrath and Sean Vitka, "Crypto War II," *Critical Studies in Media Communication* 31, no. 2 (March 15, 2014): 123–28; Daniel Oberhaus, "How the Government Is Waging Crypto War 2.0," Motherboard, August 10, 2016, https://motherboard.vice.com/en_us/article/jpgvy3/encryption-debate-the-end-of-end-to-end.

lives.[204] Terrorists have also started to adopt encryption[205] and Rob Wainwright, as the then Director of Europol, claimed that encryption presented a problem for the organisation in 75% of all investigations in 2016.[206]

Yet, as cyber attacks continue to grow in severity, encryption also provides a vital pillar of defence. The porous nature of cyberspace has led to an 'age of leaks.'[207] Important databases including Sony Pictures and the US Office of Personnel Management have been breached over the last few years with encryption crucial in mitigating the negative impact of such incidents. Although data breaches do not have an equivalent impact on the international system (when compared to 'hard' security issues such as armed conflict or nuclear proliferation), their importance should not be underestimated. Consider, for example, that the Sony data breach in 2014 became embroiled in a larger narrative related to a North Korean attack on US free speech.[208] Likewise, the leaking of DNC documents in the run-up to the US 2016 presidential election disrupted political processes and undermined institutions in the US,[209] regardless of whether the incident affected voter preferences.

Encryption therefore represents a thorny dilemma, and an issue highly relevant to some of the primary threats faced by states including cyber attacks and terrorism. It is either a positive or negative force, depending on the form of security at hand. The power of ciphers simultaneously

[204] Sir Harry Hinsley, "The Influence of ULTRA in the Second World War" (October 19, 1993); Jack Copeland, "Alan Turing: The Codebreaker Who Saved 'Millions of Lives," BBC News, June 19, 2012, http://www.bbc.co.uk/news/technology-18419691.
[205] Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9, no. 6 (June 2016): 20–25.
[206] Joseph Cox, "Encryption Gets in The Way of 75% of Cases, Europol Chief Says," Motherboard, May 10, 2016, https://motherboard.vice.com/en_us/article/4xa3jq/encryption-gets-in-the-way-of-75-of-cases-europol-chief-rob-wainwright.
[207] Richard J Aldrich and Christopher R Moran, "'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy," *Political Studies*, (March 28, 2018); Henry Farrell and Martha Finnemore, "The End of Hypocrisy: American Foreign Policy in the Age of Leaks," *Foreign Affairs* 92, no. 6 (November 2013): 22–26.
[208] Ellen Nakashima, "Why the Sony Hack Drew an Unprecedented U.S. Response against North Korea," *The Washington Post*, January 15, 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html.
[209] Thomas Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History," Esquire, October 20, 2016, https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/.

protects citizens when they send sensitive documents across the internet or as they shop online, while also providing a means for foreign spies, terrorists and criminals to remain covert.[210] It is these inherent dichotomies of encryption that drive much of the tension and fragmentation observed in the US case study.[211]

Assemblage Configuration: dispersed power and fragmented incentives

This following section outlines the relevant security actors that comprise the US Encryption Security Assemblage, as well as their incentive structures and power. A variety of security actors are involved and are classified into six traditional units (based on the theoretical model outlined in Chapter Two): corporations; government actors; international organisations and networks; knowledge, advocacy and pressure groups; media and news outlets; and academic actors.

Power is dispersed across a variety of security actors in the assemblage. This means that no single actor has achieved a decisive level of dominance and thereby able to consistently achieve its goals. This diffusion of power, combined with the variety of incentive structures that exist, have proved decisive variables in leading to a highly fractured and unstable internal assemblage processes with inconsistent security outputs

Actors are initially organised via these traditional units. This provides a useful means to assess the coherence of these categories, and the explore the tensions and disputes that exist within

[210] Moore and Rid, "Cryptopolitik and the Darknet," 7.
[211] Jamie Collier and Jantje Silomon, "Security Dichotomies in Cyber Security" (British International Studies Association 41st Annual International Conference 2016, Edinburgh, UK, 2016).

such units. Indeed, examining a variety of government actors together yields useful insights about the tensions and disputes that exist within the public sector that are too often missed.[212]

A significant source of tension in the US Encryption Assemblage comes from disputes between actors that advocate for robust encryption that cannot be accessed by anyone other than the user (referred to as strong-encryption actors) and by those that believe, by contrast, actors other than the user should be able to access encrypted data – albeit often in a limited capacity and on the basis that certain conditions are met, typically related to national security.[213] This second group of stakeholders are referred to as weak-encryption actors. Moving beyond traditional IR units and sectors, the assemblage configuration section will therefore seek to reformulate the assemblage through two interunit clusters that better capture these dynamics: strong and weak-encryption clusters.

Corporations

The overwhelming majority of corporations operating in the US are strong encryption advocates. Profit-driven technology firms represent the most prominent intra-unit cluster, comprising a variety of platforms, messaging applications, software and hardware developers including Apple, Facebook, Microsoft, Google, Twitter, etc. Profit-driven technology firms have implemented both end-to-end encryption on communication applications and introduced on-device encryption automatically.[214] The majority of phones, tablets and laptops in the US

[212] For example, a variety of publications have characterised US encryption disputes as occurring between Silicon Valley and the US government - missing critical tensions that exist within each of these communities. See, for example, Sara Sorcher, "The Battle between Washington and Silicon Valley over Encryption," CS Monitor, http://projects.csmonitor.com/cryptowars; Shanika Gunaratna, "The Snowden Effect: Silicon Valley vs. the Government," CBS News, June 6, 2016, https://www.cbsnews.com/news/the-snowden-leaks-effect-its-now-silicon-valley-vs-the-government-privacy/.

[213] Weak-encryption actors are therefore still likely to recognise the importance of encryption and are not necessarily anti-encryption per se.

[214] Brian Barrett, "The Year Encryption Won," Wired, December 23, 2016, https://www.wired.com/2016/12/year-encryption-won/; Patrick Howell O'Neill, "Android 7 Boasts New Encryption Features as the Crypto War Soldiers On," The Daily Dot, August 24, 2016,

are now encrypted by default with users unencrypting their devices as they unlock them with a passcode or thumbprint.[215]

Apple has emerged as a vocal strong-encryption advocate – a stance supported by technical underpinnings. Its devices have been encrypted by default since September 2014[216] and the firm is unable to access user data, even if ordered to do so by a court.[217] Apple has also calibrated its iteration count for entering a passcode on a device to around 80 milliseconds – meaning that it would take more than five years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.[218] To further discourage brute-force attacks, Apple devices can also be setup to automatically wipe all data after ten consecutive incorrect passcode entry attempts. End-to-end encryption has also been implemented on Apple's communication applications, including iMessage and FaceTime.[219] Other large technology firms have taken a similar approach. Google declared that it was encrypting all Gmail data that flowed between its data centres in March 2014 – a move followed a week later by Yahoo. While Google's phone software Android already offered full-device encryption as an option beforehand, it was introduced by default in September 2014.[220]

---

https://www.dailydot.com/layer8/android-nougat-encryption/.

[215] ibid.

[216] "iOS Security," (Cupertino, CA: Apple September 2014); Cyrus Farivar, "Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot," Ars Technica, September 18, 2014, https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

[217] Mathew Green, "Is Apple Picking a Fight With the U.S. Government?," Slate, September 23, 2014, http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html.

[218] "IOS Security: IOS 11" (Cupertino, CA: Apple, January 2018), https://www.apple.com/business/docs/iOS_Security_Guide.pdf;

[219] In the past, messages were still backed up to Apple's cloud (iCloud) meaning that Apple or any other actor that gained access to Apple's systems could theoretically read a user's messages. Since the launch of iOS 11, however, Apple have closed off this point of access, thereby making it even more difficult for government actors to access the personal data of Apple users. See, Christian de Looper, "Apple Is Preparing To Make iMessage App Even Safer," Digital Trends, June 9, 2017, https://www.digitaltrends.com/mobile/apple-ios-11-imessage-security/.

[220] Google briefly revised this policy due to performance concerns and then later reintroduced it by default in late 2015. See Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police," The Washington Post, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.291bfbbb3650; William Turton, "WhatsApp Rolls out End-to-End Encryption to All 1

WhatsApp, the largest messaging network in history with over 1 billion users also deployed end-to-end encryption in April 2016.[221] This move was echoed by its parent company Facebook when the social media firm rolled out 'secret conversations' to all 900 million Facebook messenger users in October 2016, ensuring that messages were encrypted from one device to another.[222] In addition to strong encryption standards, many of these private technology firms have highly sophisticated security teams that are able to assist in protecting the computers, networks and systems where encrypted data sits. Google's Project Zero, for instance, is regarded as a highly capable team of bug and vulnerability hunters that improves the security of Google applications and software, and highly respected within the industry according to one interviewee.[223] Most well-established technology firms also run bug-bounty programs that encourage security researchers to report their discoveries of bugs and vulnerabilities directly.[224]

Although likely in part due to a motivation to protect user data, it is also noticeable that various encryption initiatives have been introduced by large technology firms after Snowden leaked NSA documents. These documents revealed that large technology firms wilfully cooperated with US intelligence agencies in many instances (for example through the PRISM programme where the NSA mined data from the servers of technology firms directly).[225] Although legally compelled to do so, they did not put up the same level of resistance as has been observed since the Snowden leaks. Large technology firms were therefore markedly less concerned about

Billion Users," The Daily Dot, April 5, 2016, https://www.dailydot.com/layer8/whats-app-rolls-out-crypto-one-billion/.

[221] William Turton, "WhatsApp Rolls out End-to-End Encryption to All 1 Billion Users."

[222] Andy Greenberg, "You Can Finally Encrypt Facebook Messenger, So Do It," Wired, October 4, 2016, https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/.

[223] Interview with cyber security consultant (c) (working with UK and US Government clients) by the author. London, UK. July 2, 2018; Andy Greenberg, "Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers," Wired, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/.

[224] Dan Swinhoe, "Why More and More Companies Are Turning to Bug Bounties," IDG Connect, April 30, 2018, https://www.idgconnect.com/abstract/30307/why-companies-bug-bounties.

[225] "PRISM / US-984XN Overview, or The SIGAD Used Most in NSA Reporting Overview," National Security Agency: Special Source Operations. April 2013. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1979.dir/doc.pdf

opposing governmental access to user data when the issue received less public attention. The strong-encryption response from technology firms since the Snowden leaks is not necessarily therefore a change in ideology – more likely, there has been an acknowledgment that continued cooperation with US Government actors, (or at least the perception of cooperation), has a damaging impact on their brand and profitability with it therefore in their interests to publicly distance themselves. Although difficult to verify (given technology firm's incentive to portray their response as a principled, rather than commercial, reaction) this more pragmatic reading of the response of technology firms has both been confirmed by several interviewees[226] and reinforced by the fact that most technology firms still commercialise their users' data through the use of tailored directed advertisements. Facebook, for example, used 98 personal data points to target individual demographics including relationship status, age, the type of restaurants an individual visits and their employer.[227] Meanwhile, Google has developed a program called Customer Match where an advertiser's brand is promoted at the moment where customers have been found to be most receptive to its message.[228] It could be argued that Apple has a stronger emphasis on user privacy as its business model does not require it to sell personal information to advertisers or other organisations. It does collect user data in order to understand how users interact with its products, but does this is through a differential privacy model where the data from a number of users are collated so that analysts never view the data of specific individuals.[229]

[226] Interview with a former National Security Agency lawyer by the author. Cambridge, Massachusetts. May 31, 2017; Interview with cyber security consultant (c); Interview with a cyber security, privacy, and encryption academic.
[227] Caitlin Dewey, "98 Personal Data Points That Facebook Uses to Target Ads to You," The Washington Post, August 19, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/.
[228] Mark Hachman, "The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers," PC World, October 1, 2015, https://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html.
[229] "Apple Differential Privacy Technical Overview," Apple, https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.

The strong technical capability of these firms has also been complemented by their attempts to influence both political and public debates. Strong-encryption technology firms have significantly developed their lobbying capabilities in recent years and this has likely been a factor in the development of processes including the vulnerability equity process (VEP) – a US Government initiative that releases vulnerability information to vendors directly when appropriate.[230] Technology firms have engaged in well-known forms of corporate advocacy, including setting up policy offices in Washington and Brussels, hiring policy managers and creating the Internet Association (a trade association that advances the interest of various technology firms).[231] Technology firms now outspend banks two to one on lobbying in the US.[232] Facebook's spending on lobbying has climbed from $1,350,000 in 2011 to $11,510,000 in 2017.[233] Meanwhile, Google's parent company Alphabet parted with $18,140,000 for lobbying in 2017 – more than any other individual firm in the US.[234] The 'revolving door' phenomenon has occurred in the technology sector[235] where government employees leave their jobs in government to become lobbyists, providing their new employer with unique insight and access into government operations.[236] Google typifies this process[237] with their former policy

[230] Technology firms have campaigned for a more stringent VEP process. For example, see Brad Smith, "The Need for a Digital Geneva Convention," Microsoft, *Microsoft on the Issues* (blog), February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.
[231] Mikkel Flyverbom, "Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations," in *Power, Policy and Profit: Corporate Engagement in Politics and Governance*, ed. Christina Garsten and Adrienne Sörbom (Cheltenham, UK: Edward Elgar Publishing, 2017), 115-133. pp. 122.
[232] Olivia Solon and Sabrina Siddiqui, "Forget Wall Street – Silicon Valley Is the New Political Power in Washington," The Guardian, March 11, 2017, https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington.
[233] "Lobbying Spending Database - Facebook Inc," OpenSecrets, accessed March 2, 2018, https://www.opensecrets.org/lobby/clientsum.php?id=D000033563&year=2017.
[234] "Lobbying Spending Database," OpenSecrets, accessed March 28, 2018, https://www.opensecrets.org/lobby/top.php?showYear=2017&indexType=s.
[235] Cecilia Kang and Juliet Eilperin, "Why Silicon Valley Is the New Revolving Door for Obama Staffers," The Washington Post, February 28, 2015, https://www.washingtonpost.com/business/economy/as-obama-nears-close-of-his-tenure-commitment-to-silicon-valley-is-clear/2015/02/27/3bee8088-bc8e-11e4-bdfa-b8e8f594e6ee_story.html; Seth Fiegerman, "Obama's Staff Is Taking over Silicon Valley," CNN Money, August 11, 2016, http://money.cnn.com/2016/08/11/technology/obama-staff-silicon-valley/index.html.
[236] Jeffrey Lazarus, Amy McKay and Lindsey Herbel, "Who Walks Through the Revolving Door? Examining the Lobbying Activity of Former Members of Congress," *Interest Groups & Advocacy* 5, no. 1 (January 2016): 82-100. pp. 82-83; Beth L Leech, *Lobbyists at Work* (New York: Apress, 2013).
[237] Megan Crouse, "Tech Companies Lobby for Security, National Trade," ECN, April 28, 2015, https://www.ecnmag.com/article/2015/04/tech-companies-lobby-security-national-trade.

director Andrew McLaughlin taking up a position in the Obama administration as the Deputy Chief Technology Officer of the United States and with 100 of Google's 124 lobbyists (in 2017) having previously held US Government jobs.[238] Meanwhile, Facebook has hired people who have worked on strategic communications for the National Security Council, trade policy and judicial nominations.[239] Strong-encryption actors also influence political and public debates via other means. Technology firms typically fund research and build relationships between technology firms, universities and other organisations involved in encryption topics.[240] Google offers a policy fellowship that funds students to spend time with policy-based organisations, many of whom are proponents of strong-encryption including the Electronic Frontier Foundation (EFF), the Open Technology Institute and the Reporters Committee for Freedom of the Press.[241] It also has significant influence over the think tank New America[242] that has previously published on the importance of strong-encryption.[243]

Ideologically-motivated technology firms represent the second intra-unit cluster of corporations, that have put user privacy at the centre of their products and services as they were created. As consumers have become increasingly concerned about hacking and government surveillance, communication applications that brand themselves as secure and committed to preserving users' privacy with strong encryption have become increasingly popular.[244] This

[238] Mikkel Flyverbom, "Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations," 124.
[239] Hannah Kuchler, "Why Obama's West Wingers Went West," Financial Times, January 10, 2018, https://www.ft.com/content/56712806-f58f-11e7-88f7-5465a6ce1a00.
[240]Mikkel Flyverbom, "Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations," 124.
[241] "Google Policy Fellowship," Google, https://www.google.com/policyfellowship/hosts.html.
[242] Google funds New America. New America also fired an employee after he criticised Google. See, Kenneth P Vogel, "Google Critic Ousted From Think Tank Funded by the Tech Giant," The New York Times, August 30, 2017, https://www.nytimes.com/2017/08/30/us/politics/eric-schmidt-google-new-america.html; Kenneth P. Vogel, "New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic," The New York Times, September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.
[243] "Promoting a Secure Internet," New America, https://www.newamerica.org/oti/promoting-secure-internet/; "Read This Before You Rail Against Encryption," New America, /weekly/101/read-this-before-you-rail-against-encryption/.
[244] Jeff John Roberts, "Here Are the Most Popular Apps for Secure Messages," Fortune, January 17, 2017,

included messaging applications Telegram, Line, Cyber Dust, Proton Mail and Signal (which was endorsed by Snowden).[245] Unlike the commercially motivated technology firms outlined above, the incentives of this second group of encryption actors is predominately ideological with many even operating on a not-for-profit basis[246] – highlighting the variety of incentive structures that exist within contemporary cyber security assemblages. For instance, Signal has never taken venture capital funding or sought investment due to fears that becoming a profit-driven firm could risk compromising its privacy values.[247] Of course, this is not to say that profit-motivated technology firms are devoid of ideological principles – however, the distinction between the groups remains coherent given their significantly different stances on privacy issues. Crucially, profit-motivated technology firms appear to have largely implemented encryption for business reasons[248] while ideologically-motivated technology firms have largely implemented encryption out of principle.

This second cluster is also emblematic of power diffusion processes ongoing in cyber security and clearly observed in this case study.[249] The low barriers to entry for producing robust encryption algorithms gives strong-encryption actors an inherent advantage in the context of material power. The messaging application Signal represents a good example of this. Signal's encryption protocol is widely respected and has been integrated into a variety of mainstream communication applications including Google, Facebook, Skype and WhatsApp.[250] Despite

---

http://fortune.com/2017/01/17/most-popular-secure-apps/; James Martin, "Encrypted Messaging Apps," CNET, March 23, 2016, https://www.cnet.com/uk/pictures/timeline-a-history-of-encryption-and-government-backdoors-pictures/9/.

[245] Edward Snowden. Twitter post. November 2, 2015. https://twitter.com/Snowden/status/661313394906161152.

[246] "Pricing," ProtonMail, accessed March 28, 2018, https://protonmail.com; "Telegram F.A.Q.," Telegram, accessed March 28, 2018, https://telegram.org/faq.

[247] Brian Acton, "Signal Foundation," Signal, February 21, 2018, https://signal.org/blog/signal-foundation/.

[248] Shown by the sharp uptake of encryption the aftermath of the Snowden documents, when their reputations were effected, yet not implementing it before. See, Interview with a former National Security Agency lawyer; Interview with a cyber security, privacy, and encryption academic.

[249] Joseph S Nye Jr, *The Future of Power*.

[250] Joshua Lund, "Signal Partners with Microsoft to Bring End-To-End Encryption to Skype," Signal, January 11, 2018, https://signal.org/blog/skype-partnership/.

such widespread adoption, the resources of the non-profit organisation are decisively small: as of February 2018, there have only been an average of 2.3 full-time software developers and the entire Signal team has never been more than seven people.[251] It is these low barriers to entry that are one reason why cyber security assemblages have tended to comprise such a variety of actors. Signal's influence in the US shows that even actors with very limited resources can nonetheless have a significant impact on both security and politics.

Whilst the majority of technology firms have introduced and publicly advocated for strong-encryption (either for commercial or ideological reasons), not all technology firms have incentives to support strong encryption. The final intra-unit corporation cluster is therefore weak-encryption technology firms – that is the corporations that actively profit by breaking encryption or finding backdoors that allow them to get around strong encryption in other ways. It was not the FBI, but a third-party contractor that eventually unlocked the iPhone connected to the San Berindino case.[252] The sensitivity of the incident means that details of the contractor are not publicly available; however, it is widely believed that the firm that cracked the iPhone was Israeli-based firm Celebrite who have a sole-source contact with the FBI specifically to help with mobile forensics and data extraction since 2013.[253] In February 2018, it was even claimed that Cellebrite had found a way to unlock almost every iPhone on the market.[254] Although Apple then implied its latest software update would keep users secure,[255] it is

[251] Brian Acton, "Signal Foundation."
[252] Joel Rubin, James Queally, and Paresh Dave, "FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle With Apple, For Now," Los Angeles Times, March 28, 2016, http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.
[253] Ashley Carman, "An Israeli Company Is Reportedly Helping the FBI Crack the San Bernardino iPhone," The Verge, March 23, 2016, https://www.theverge.com/2016/3/23/11290374/apple-iphone-fbi-encryption-crack-cellebrite; Alina Selyukh, "The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?"
[254] Thomas Fox-Brewster, "The Feds Can Now (Probably) Unlock Every iPhone Model In Existence – UPDATED," Forbes, February 26, 2018, https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#6dc73b17667a.
[255] Tom Spring, "Apple Tackles Cellebrite Unlock Claims, Sort Of," Threatpost, February 27, 2018, https://threatpost.com/apple-tackles-cellebrite-unlock-claims-sort-of/130111/.

nonetheless clear that various contractors such as Cellebrite have the ability to break encryption and access devices at certain periods, and that such a capability is made available to intelligence and law enforcement actors. Celebrite, is part of a much larger surveillanceware market[256] that comprises a variety of firms that work closely with US Government actors in order to access technologies including other versions of encrypted iPhone,[257] the Tor Browser,[258] and encrypted messaging applications.[259]

Government actors

The most significant intra-unit cluster that sits within the US Government is that of the security and intelligence community, comprised of weak-encryption actors.[260] As a SIGINT agency, the NSA's primary mission is to intercept electronic communications. The agency has a culture of collecting SIGINT en masse[261] – a process that requires the agency to bypass encryption easily – and has invested significant resources into developing the technical resources to achieve this outcome. As a former NSA official claimed in an interview, the challenge for the agency has

[256] ibid.
[257] Joseph Cox, "Documents Prove Local Cops Have Bought Cheap iPhone Cracking Tech," Motherboard, March 9, 2018, https://motherboard.vice.com/en_us/article/xw5bqz/documents-prove-local-cops-have-bought-cheap-iphone-cracking-tech.
[258] Joseph Cox and Lorenzo Franceschi-Bicchierai, "How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of," Motherboard, February 7, 2018, https://motherboard.vice.com/en_us/article/8xdayg/iphone-zero-days-inside-azimuth-security.
[259] Joseph Cox, "Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware," Motherboard, March 7, 2018, https://motherboard.vice.com/en_us/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team.
[260] This intra-unit cluster works together, with broadly similar (albeit not identical incentive structures). This cluster formed an interagency working group during the Obama administration that outlined possible ways to guarantee access to encrypted data, including mandating companies to add backdoors; a requirement to build hardware that included ports only accessible with a law enforcement tool; and the implementation of a split-key approach where US government actors hold part of the key. See, Andrea Peterson and Ellen Nakashima, "Obama Administration Explored Ways to Bypass Smartphone Encryption," The Washington Post, September 24, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html; "Read the Obama Administration's Draft Paper on Technical Options for the Encryption Debate," The Washington Post, accessed February 8, 2018, https://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/.
[261] Stephen Budiansky, *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union* (New York: Alfred A. Knoff, 2016).

changed from just tracking already identified suspects to now spending significantly more time seeking to identifying suspects in the first place – a shift that has reinforced the importance of collecting SIGINT at a significant scale.[262] The Snowden documents point to various programmes that illustrate how this has been achieved. The NSA previously spent $250 million a year on the BULLRUN programme that was able to make significant breakthroughs in accessing data, though either hacking into target computers to access messages before they were encrypted, pressing technology firms to hand over encryption keys, or building backdoors in products.[263] The NSA has also developed the PRISM programme, a tool used to collect private data from major internet services including Gmail, Facebook and Outlook prior to its encryption.[264] Through court orders, the PRISM programme allowed the NSA to request data on specific people and access to the servers of technology firms.[265] Alongside PRISM, the NSA also sought to deliberately weaken international encryption standards with a goal of the agency's 2013 budget request to 'influence policies, standards and specifications for commercial public key technologies.'[266] The agency, is however, markedly more constrained in influencing public debate – given its role as a clandestine agency. For agencies including the NSA and CIA, it is not their job to debate what their role should be with their remit and powers decided by the executive and elected officials. As NSA Director claimed, albeit in a context outside the encryption debate 'I'm an operational commander – not a policymaker.'[267]

[262] Interview with a former National Security Agency lawyer.
[263] James Ball, Julian Borger, and Glenn Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." The Guardian, September 6, 2013. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Nicole Perlroth, Jeff Larson, and Scott Shane. "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," The New York Times, September 5, 2013. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2.
[264] T C Sottek and Janus Kopfstein. "Everything You Need to Know About PRISM," The Verge, July 17, 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.
[265] ibid.
[266] Nicole Perloth, Jeff Larson, and Scott Shane. "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."
[267] Steve Turnham, "NSA Chief Says Trump Has Not Directed Him to Counter Russian Meddling," ABC News, February 27, 2018, http://abcnews.go.com/Politics/nsa-chief-trump-directed-counter-russian-meddling/story?id=53393061.

While the NSA possesses the most impressive technical capability in accessing encrypted data[268] within the US Encryption Security Assemblage (and arguably in the world), its incentive structures are frequently misunderstood. The widespread implementation of encryption in the US by both profit and ideologically technology firms does not necessarily contradict the NSA's interests. The BULLRUN programme shows that the NSA has a previous record of breaking encryption protocols themselves – potentially providing the agency with a relative advantage if other intelligence agencies are unable to do so. The NSA seeks to gather foreign intelligence, meaning that its capability is channelled predominantly towards accessing the systems and devices commonly used by foreign targets, rather than those popular in the US (such as iPhones).[269] The NSA is also able to gather intelligence via other means – the metadata of encrypted files and devices can still yield important insights for example.[270] Further, the NSA seeks to gather intelligence covertly. The agency is therefore not interested in a public battle with technology firms and other strong-encryption actors. If and when the NSA is able to access encrypted data of software and devices popular in the US, it would instead be incentivised to keep such developments covert so as to not reveal its capability to adversaries.

The Central Intelligence Agency (CIA) is the US foreign intelligence service, tasked with gathering, processing and analysing national security information from around the world, primarily through the use of human intelligence (HUMINT). While the CIA's focus on HUMINT means the agency has less of a stake in encryption when compared to security and intelligence actors where SIGINT is more vital (including the NSA and FBI), the CIA has

[268] Based on the author's assessment having reviewed sourced material from both agencies. See, "Snowden Surveillance Archive," Snowden Archive, accessed June 22, 2018, https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi; "Vault 7: CIA Hacking Tools Revealed," WikiLeaks, March 7, 2017, https://wikileaks.org/ciav7p1/?

[269] Jenna McLaughlin, "NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says," *The Intercept*, June 10, 2016, https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/.

[270] Iain Thomson, "Cops Hate Encryption but the NSA Loves It When You Use PGP," The Register, January 27, 2016, https://www.theregister.co.uk/2016/01/27/nsa_loves_it_when_you_use_pgp/.

nonetheless demonstrated the intent to access encrypted devices in some capacity. CIA documents leaked by WikiLeaks confirm this much,[271] with the CIA's Mobile Devices Branch having developed various initiatives to access communication platforms via compromised smartphones.[272] However, compared to both the NSA and FBI, the CIA has pursued much more targeted means of intrusion, likely focused on a small number of human targets, rather than through a desire to collect intelligence at scale.[273] It should be noted that there is considerably less publicly available information on the CIA's stance, intent and capabilities in regard to encryption however.

While the FBI sits in the intelligence community, it also differs in its incentives and the agency should be seen as both an intelligence agency and a law enforcement actor in the context of encryption (indeed, the law enforcement community represents another intra-unit cluster that also comprises the Department of Justice as well as federal and state courts). The FBI has an opposition to widespread and strong encryption.[274] Whilst gathering intelligence is important to the FBI's mission, the agency is primarily a law enforcement actor that sits within the Department of Justice. This distinction between purely intelligence-gathering agencies (such as the NSA and CIA) and law-enforcement actors has implications for an actor's incentives. Compared to intelligence gathering, the FBI is primarily tasked with producing evidence that is admissible in court. While the agency has previously sought to produce evidence without

[271] "Vault7," WikiLeaks, March 7, 2017, https://wikileaks.org/ciav7p1/.
[272] Sam Biddle and Micah Lee, "The CIA Didn't Break Signal or WhatsApp, Despite What You've Heard," The Intercept, March 7, 2017, https://theintercept.com/2017/03/07/the-cia-didnt-break-signal-or-whatsapp-despite-what-youve-heard/.
[273] "Vault 7: CIA Hacking Tools Revealed," WikiLeaks, March 7, 2017, https://wikileaks.org/ciav7p1/?; "Weeping Angel (Extending) Engineering Notes," WikiLeaks, accessed June 25, 2018, https://wikileaks.org/ciav7p1/cms/page_12353643.html.
[274] Interview with 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) by the author. Skype. March 20, 2018.

accessing encrypted data,[275] the FBI has increasingly adopted a tougher stance on the issue[276] (as seen in their public dispute with Apple discussed in more detail as an exemplar below). FBI Director Christopher Wray more recently reopened this debate in January 2018, stating that law enforcement's struggle to access data on encrypted devices was an 'urgent public safety issue.'[277] The FBI has therefore become a vocal advocate of weak-encryption as it seeks to use encrypted data as evidence in court. As one interviewee who has extensively covered contemporary encryption issues highlighted, while the NSA and CIA favour covert means of accessing encrypted data, the FBI, by contrast, seeks to achieve a more public and systemic approach.[278] When the FBI uses exploits and vulnerabilities to access encrypted data, it will quickly degrade such individualised solutions as they are publicised throughout the courts. This enables strong-encryption actors to understand how their encrypted data was accessed and provides them with an opportunity to patch their systems to prevent future access.[279] Accessing encrypted data through exploits therefore provides short-term and inconsistent access and is ultimately expensive – especially when the FBI assists local police units with more limited resources.[280] The FBI is instead incentivised to develop legal mechanisms that allow them to

[275] For example, discussing the Going Dark Programme at a House Judiciary Committee in 2011, the then FBI General Counsel Valerie Caproni stated that 'addressing the Going Dark problem does not require fundamental changes in encryption technology. We understand that there are situations in which encryption will require law enforcement to develop individualized solutions.' The Going Dark programme instead sought to correct the gap through a range of techniques including attempts to ''utilize innovative technology; foster cooperation with industry; and assist our state, local, and tribal law enforcement partners in a collaborative effort to close the growing gap between lawful interception requirements and our capabilities.' See, Valerie Caproni, "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security," Washington, D.C. February 17, 2011; Jennifer Lynch, "Newly Released Documents Detail FBI's Plan to Expand Federal Surveillance Laws," Electronic Frontier Foundation, February 16, 2011. https://www.eff.org/deeplinks/2011/02/newly-released-documents-detail-fbi-s-plan-expand.

[276] This was clearly seen in 2012 when the FBI prepared draft legislation that would form email providers, voice and video chat internet service operators, instant messaging clients and social networks to modify their services to ensure that they were wiretap-friendly. See, Declan McCullagh, "FBI: We Need Wiretap-Ready Web Sites – Now," CNET, May 4, 2012. https://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/.

[277] Christopher Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation," presented at the FBI International Conference on Cyber Security, Fordham University, New York, January 9, 2018, https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

[278] Interview with a cyber security journalist by the author. May 24, 2018. London, UK

[279] ibid.

[280] Interview with Adam Segal.

access encrypted data with more certainty and consistency – such as through compelling technology firms to assist them in the process.

The FBI has been unusually public in seeking to achieve its aims – as observed in their public dispute with Apple (which will be discussed as a bounded case study example in the assemblage dynamics section). Legal disputes between the FBI and corporations usually take place under seal in national security courts such as the Foreign Intelligence Surveillance Act courts, meaning that the public never knows about the proceedings and outcomes.[281] Yet, the Apple-FBI dispute took place in a Californian public court.[282] EFF attorney Andrew Crocker has suggested that this was an intentional tactic by the FBI.[283] Filing in a public court brought the encryption standoff to a head. This would suit the FBI if it was confident of winning the public debate. Even if the FBI lost the court battle, if they were able to develop a convincing narrative that technology firms were aiding and abetting terrorism and serious crime that held political weight, Congress would be more likely to pass a law requiring technology firms to comply with aggressive decryption requests.[284]

The FBI sits under the jurisdiction of the Department of Justice. Typically faced with convergent incentive structures, other law-enforcement actors naturally assist the FBI. If law enforcement intelligence agencies struggle to investigate crime and terrorism as a result of encryption, it becomes more difficult for both state, federal and jurisdiction attorney offices to prosecute potential guilty parties. Central attorney actors have therefore also sought to pressurise technology firms. Attorney General Jeff Session accused technology companies of failing to adequately assist federal investigations access encrypted devices and

[281] Mark Sullivan, "Why The FBI Chose To Try The Apple Encryption Case In The Media," Fast Company, February 22, 2016, https://www.fastcompany.com/3057033/why-the-fbi-chose-to-try-the-apple-encryption-case-in-the-media.
[282] Eileen M Decker et al., In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203.
[283] Mark Sullivan, "Why The FBI Chose To Try The Apple Encryption Case In The Media."
[284] ibid.

communications, claiming that the FBI was blocked from accessing nearly 7,500 mobile devices in 2017 (although the number was in fact under 2,00 although the inflated figure was deemed to be accidental).[285] This stance was reinforced by the Deputy Attorney General Rod Rosenstein who called for 'responsible encryption' that 'that allows access only with judicial authorization.'[286] These efforts have also been supported by local law-enforcement actors. Nine separate court jurisdictions have challenged Apple's encryption stance including New York (both Southern and Eastern district), Illinois, California (both Northern and Southern District) and Massachusetts.[287] These state-level courts have often emphasised different reasons for challenging encryption. For example, the New York proposal cited terrorism as a threat necessitating the legislation, while the California bill mentioned human trafficking.[288] City jurisdictions have also been active on the issue. Manhattan District Attorney Cyrus Vance Jr has been a vocal critic and campaigned for against strong-encryption for instance.[289]

Unlike intelligence and law enforcement actors, the State Department has been a supporter of strong-encryption given its efforts to promote internet freedom and enable dissent abroad. The State Department's Bureau of Democracy, Human Rights and Labour (DRL) seeks to 'advance

[285] Thuy Ong, "The FBI inflated the number of encrypted phones linked to crime," The Verge, May 23, 2018, https://www.theverge.com/2018/5/23/17383496/fbi-encrypted-phones-inflated-number-crime; interview with a cyber security journalist; Sarah N Lynch and Brendan Pierson, "U.S. Attorney General Says Tech Companies Should Help Access Encrypted Evidence," Reuters, November 2, 2017, https://www.reuters.com/article/us-usa-justice-encryption/u-s-attorney-general-says-tech-companies-should-help-access-encrypted-evidence-idUSKBN1D21V2.
[286] Rod J Rosenstein, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy," The United States Department of Justice, October 10, 2017, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.
[287] Jenna McLaughlin, "New Court Filing Reveals Apple Faces 12 Other Requests to Break Into Locked iPhones," The Intercept, February 23, 2016, https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.
[288] Eric Geller, "California Lawmaker Introduces Human-Trafficking Bill That Bans Strong Encryption," The Daily Dot, January 21, 2016, https://www.dailydot.com/layer8/california-encryption-backdoors-legislation-human-trafficking/.
[289] Cyrus R Vance, Jr, "Cybersecurity and U.S. National Security," § United States Senate Committee on Armed Services (2016), https://www.armed-services.senate.gov/imo/media/doc/Vance_07-14-16.pdf; Cyrus R Vance, Jr, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," § United States Senate Committee on the Judiciary (2015), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf.

the exercise of human rights and fundamental freedoms online through a diverse set of Internet freedom policy and programming activities'[290] and this includes US Government funding for strong encryption solutions to address restrictions and limitation on access to online information.[291] For example, it has supported the use of encryption tools used by 'LGBT activists in eastern Europe and central and southern Africa, democracy activists in Ethiopia and Turkey, and journalists in Egypt and Nicaragua.'[292] In 2013, the State Department and the United States Agency for International Development (USAID) awarded $25 million to civil society groups working to advance 'Internet Freedom' policy initiatives.[293] A State Department spokesperson told the Wall Street Journal that an unspecified portion of that $25 million was being used to develop secure communications tools.[294] However, despite its support of strong-encryption, the State Department has stayed largely silent in recent encryption debates.[295] This is because in addition to its own incentives, the State Department also has a responsibility to represent the entirety of the US Government abroad.[296] Here, it is not only the stance of the weak-encryption actors outlined above that are important, but the stance of central government actors, such as Congress and the executive, that have struggled to develop a coherent position on encryption as shown below.

Other government actors support strong encryption (albeit with a less pubic stance on the issue). This includes the Department for Commerce that prioritises economic growth and trade,

[290] "Internet Freedom," U.S. Department of State, accessed March 29, 2018, https://www.state.gov/j/drl/internetfreedom/index.htm.
[291] Wolfgang Schulz and Joris van Hoboken, "Human Rights and Encryption" (Paris, France: UNESCO, 2016), http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.
[292] Chris Bing, "Why Is State Department Silent in the Global Encryption Debate?," *Fedscoop*, June 24, 2016, https://www.fedscoop.com/should-the-state-department-be-more-involved-in-the-encryption-debate/.
[293] ibid.
[294] Damian Paletta, "How the U.S. Fights Encryption–and Also Helps Develop It," The Wall Street Journal, February 22, 2016, https://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096.
[295] Chris Bing, "Why Is State Department Silent in the Global Encryption Debate?"
[296] ibid.

where encryption can help to protect the security of financial data and transactions.[297] The National Institute of Standards and Technology also promotes US innovation and industrial competitiveness and has published guidelines for strong-encryption standards in order to promote cyber security.[298]

Congress has displayed limited degrees of support for both strong and weak-encryption policy proposals with the issue in political gridlock. In November 2015, two Senate and two House committees began to review encryption, seeking to develop a congressional backlash to strong encryption technologies in the wake of a terrorist incident in Paris that killed 130 people.[299] In the Senate, Chairman of the Senate Armed Services Committee John McCain called unrestricted encryption 'unacceptable' and announced 'In the Senate Armed Services [Committee] we're going to have hearings on it and we're going to have legislation.'[300] His comments were echoed by Richard Burr, head of the Senate Intelligence Committee who launched a review of encryption, claiming that 'if it means that people are going to have to change their business models, then so be it,' indicating that the move could lead to significant change.[301] In the House meanwhile, Homeland Security Committee Chairman Mike McCaul claimed that 'The biggest threat today is the idea that terrorists can communicate in dark space, dark platforms, and we can't see what they're saying.'[302] House Intelligence Committee

[297] Interview with Adam Segal.
[298] Interview with Adam Segal; Elaine B. Barker, "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms" (Gaithersburg, MD: National Institute of Standards and Technology, August 2016).
[299] Danny Yadron, Alistair Barr, and Daisuke Wakabayashi, "Paris Attacks Fan Encryption Debate," Wall Street Journal, November 20, 2015, sec. Tech, http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407; Brian Krebs, "Paris Terror Attacks Stoke Encryption Debate," Krebs on Security, November 17, 2015, https://krebsonsecurity.com/2015/11/paris-terror-attacks-stoke-encryption-debate/.
[300] Eric Geller, "Congress Plans Encryption Investigations as Paris Attacks Reignite 'Crypto Wars,'" The Daily Dot, November 18, 2015. https://www.dailydot.com/layer8/encryption-backdoors-congress-investigations-surveillance-paris-attacks/.
[301] Eric Geller, "Congress Plans Encryption Investigations as Paris Attacks Reignite 'Crypto Wars.'"
[302] Eric Geller, "Heads of 2 Powerful House Committees Join Anti-Encryption Crusade," The Daily Dot, December 11, 2015, https://www.dailydot.com/layer8/encryption-backdoors-terrorism-surveillance-congress-house-chairmen/.

Chairman Devin Nunes claimed that terrorists have 'gotten very good at hiding from intelligence services around the globe' as a result of the technology they use.[303]

Congress has also proposed strong-encryption initiatives. Chairman of the Senate Homeland Security Committee, Ron Johnson broke with the Republican party line when he criticised the use of backdoors in January 2016, arguing that backdoors 'could do more harm than good' and that support for them came from 'just not understanding' the complexity of the issue,[304] using similar arguments to civil libertarians and cryptographers. He argued that anti-encryption laws would likely only push terrorists onto foreign-based platforms and communication platforms that are outside of the US Government's control. In a separate initiative shortly after, two House lawmakers introduced a bill to prevent states from regulating or controlling the kind of encryption that technology firms were able to use.[305] The bill states that no company could require or even ask a company to 'have the ability to decrypt or otherwise render intelligible information that is encrypted or otherwise rendered unintelligible using its product or service.'[306] Given that both strong and weak-encryption initiatives have been proposed through Congress, it is clear that there is significant divergence within the US government legislature, perhaps highlighting the diverging incentive structures of elected officials and the variety of opinions within the various constituencies of the US that they represent.

The executive branch of the US Government has also taken a balanced view, neither fully endorsing strong nor weak-encryption. This is likely to be due to both the need to balance the variety of incentives that exist within the US Government as well as the variety of views held by the electorate more broadly. President Barack Obama, for instance, adopted a middle-

[303] ibid.
[304] Eric Geller, "Senate Homeland Security Chairman: Encryption Law Could 'Do More Harm Than Good,'" The Daily Dot, January 28, 2016, https://www.dailydot.com/layer8/encryption-ron-johnson-backdoors-crypto-wars-aei-event/.
[305] As of February 2018, it has yet to be confirmed whether the bill will be approved and make it into law
[306] Ted Lieu, "To Preempt State Data Security Vulnerability Mandates and Decryption Requirements.," Pub. L. No. 4528 (2016).

ground position arguing that 'you cannot take an absolutist view on this' and went on to discuss how civil liberties have required compromise to ensure Americans are able to live in a safe society where law enforcement can prevent activities including terrorism, child pornography and tax evasion.[307] The former President stated that the strong encryption stance taken by technology firms is 'fetiszhing our phones above every other value. And that can't be the right answer.' Obama argued a better alternative would be to 'create a system where encryption is as strong as possible. The key is secure as possible, it is accessible by the smallest number of people possible for a subset of issues that we agree are important.'[308] The problem with Obama's argument, however, is that it does not directly address the stance taken by technology firms that argue such a system is technically impossible as enabling providing access to communications for certain government actors would inevitably undermine security more broadly. Obama even acknowledged that 'how we design that is not something that I have the expertise to do.'[309]

The ambiguity of Obama's stance was also reflected in his administration's response to a petition supporting encryption. In the US, a petition requires 100,000 signatures to warrant an official response. Yet, in its initial response more than a month after the petition reached 100,000 signatures, the White House avoided commenting substantively on the issue and merely promised to meet with the activities who launched the campaign.[310] Attendees at that meeting a few days later told reporters that the White House was poised to say more in the coming weeks – a senior administration official even promised "a more fulsome response soon."[311] Yet, no further statement related to the petition ever arrived. Beyond such public

[307] Barack Obama, "Remarks by the President at South By Southwest Interactive" (March 11, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive.
[308] ibid.
[309] ibid.
[310] Eric Geller, "White House Ducks Petition's Demand for Strong Encryption," The Daily Dot, December 9, 2015, https://www.dailydot.com/layer8/white-house-encryption-backdoors-petition-response/.
[311] ibid.

statements, the Obama administration has responded ambiguously to encryption in its policy stance. Obama has stopped short of calling for or promoting legislation to curb encryption. Yet while attempts to mandate technology firms to build backdoors into their services or weaken encryption have not occurred. The administration has instead sought to persuade companies that have moved to encrypt their customers' data to create ways for the government to still access data relevant for criminal and terrorism investigations.[312] In this regard, the Obama administration's strategy was to apply pressure informally – although details of this process and its extent are unclear given the secretive nature of such interactions.

It initially appeared that the Executive's encryption stance would change with the election of President Donald Trump. One interviewee even suggested that Obama effectively 'kicked the can down the road' in regards to leaving the issue unresolved for the next President to address.[313] At the time of the Apple-FBI dispute, Trump argued that the FBI should be able to access the San Bernardino shooter's phone. Speaking about the federal court order that sought to require Apple to help the FBI break into San Berindino shooter Farook's iPhone, Trump claimed 'I agree 100% with the courts…In that case, we should open it up. I think security over all – we have to open it up, and we have to use our heads.'[314] During the presidential election campaign, Trump signalled a more hostile approach to Apple than his predecessor arguing that 'Apple ought to give the security for that phone, OK. What I think you ought to do is boycott Apple until such a time as they give that security number. How do you like that? I just thought of it. Boycott Apple.'[315] Trump also claimed that Apple's response was for political reasons

[312] Rainey Reitman, "Partial Victory: Obama Encryption Policy Rejects Laws Mandating Backdoors, But Leaves the Door Open for Informal Deals," Electronic Frontier Foundation, October 9, 2015, https://www.eff.org/deeplinks/2015/10/partial-victory-obama-encryption-policy-reject-laws-mandating-backdoors-leaves.
[313] Interview with Adam Segal.
[314] David Wright, "Donald Trump: Apple Should Hack San Bernardino Phone," CNN, February 17, 2016, https://edition.cnn.com/2016/02/17/politics/donald-trump-apple-encryption-debate/.
[315] Jeremy Diamond, "Donald Trump Calls for Apple Boycott," CNN, February 20, 2016, https://edition.cnn.com/2016/02/19/politics/donald-trump-apple-boycott/index.html.

claiming that 'Tim Cook is looking to do a big number, probably to show how liberal he is.'[316] Trump's threat to boycott Apple was also made via his Twitter account where he tweeted on the same day 'I use both iPhone & Samsung. If Apple doesn't give info to authorities on the terrorists I'll only be using Samsung until they give info.'[317] Yet, beyond such campaign rhetoric, the Trump's administration has been characterised predominantly by inaction. The administration has not launched any new encryption bills nor sought to mandate technology firms to allow government access – indicating a decision to maintain continuity with previous encryption policy. As of 2017, President Trump uses an iPhone exclusively.[318]

International Organisations and Networks

The US intelligence community works closely with ally states within the Five Eyes alliance that also includes Australia, Canada, New Zealand and the UK. Intelligence agencies in these other states have a similar set of incentive structures, and thereby take a similar line on encryption. The alliance thereby provides an opportunity for different intelligence agencies to collaborate on the issue at an international level. A meeting in Ottawa in June 2017 reflected this where encryption was discussed as a key issue. The Australian delegation saying publicly that they intended to 'thwart the encryption of terrorist messaging.'[319]

Out of the other four Five Eyes members, the NSA has worked most closely with the UK's GCHQ on a bilateral level, as revealed by NSA and GCHQ Snowden documents. The two intelligence agencies have long enjoyed a close relationship[320] and this is reflected in various

[316] ibid.
[317] ibid.
[318] Rich McCormick, "Donald Trump Is Using an iPhone Now," The Verge, March 29, 2017, https://www.theverge.com/2017/3/29/15103504/donald-trump-iphone-using-switched-android.
[319] Chris Duckett, "Australia Will Lead Five Eyes Discussions to 'Thwart' Terrorist Encryption: Brandis," ZD Net, June 26, 2017, http://www.zdnet.com/article/australia-will-lead-five-eyes-discussions-to-thwart-terrorist-encryption-brandis/.
[320] Interview with a former National Security Agency lawyer; Aldrich, *GCHQ*; Hayden, Michael. Playing to the Edge: American Intelligence in the Age of Terror, New York: Penguin Press, 2016.

Snowden documents[321] as well as GCHQ's annual investment portfolio that revealed that the NSA has paid GCHQ over £100 million in return for assistance in various capacities.[322] On the issue of encryption specifically, the NSA has worked with GCHQ in order to bypass standards. An operation with the cover name MUSCULAR that was part of WINDSTOP, a joint NSA-GCHQ program involved the intelligence agencies breaking into the main communication links that connect Yahoo and Google data centres around the world.[323] In an NSA presentation slide, the process is shown to take place at the Google Front End server (where the internal Google cloud meets the public internet) with encryption added and removed at this point, thereby providing an opportunity for intelligence agencies to obtain plaintext or unencrypted data.[324] Given that these agencies have front-door access to Google and Yahoo through the PRISM program, MUSCULAR has been viewed as unusually aggressive with the sort of capability used typically reserved for spying on foreign adversaries (rather than US companies).[325]

---

[321] "Special Source Operations: The Cryptographic Provider of Intelligence from Global High-Capacity Telecommunications Systems" National Security Agency, accessed April 27, 2018, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH5098.dir/doc.pdf; "BULLRUN: PTF Lead for Special Operations and Policy," Government Communications Headquarters, accessed April 27, 2018, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0189/b2203e23.dir/doc.pdf.

[322] The details of the NSA payments, and the influence the US has over Britain, are set out in GCHQ's annual "investment portfolios". The papers show that the NSA gave GCHQ £22.9m in 2009. The following year the NSA's contribution increased to £39.9m, which included £4m to support GCHQ's work for NATO forces in Afghanistan, and £17.2m for the agency's Mastering the Internet project, which gathers and stores vast amounts of "raw" information ready for analysis. The NSA also paid £15.5m towards redevelopments at GCHQ's sister site in Bude, north Cornwall, which intercepts communications from the transatlantic cables that carry internet traffic. See, Nick Hopkins and Julian Borger, "Exclusive: NSA Pays £100m in Secret Funding for GCHQ," The Guardian, August 1, 2013, https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

[323] "2013 U.S. Intelligence Black Budget: Foreign Partner Access Project. United States Intelligence Community," 2013, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHe7fe.dir/doc.pdf. pp. 61-64; Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," The Washington Post, October 30, 2013. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.f22c4898ed97.

[324] Gellman and Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say."

[325] ibid.

Knowledge, Advocacy, and Pressure Groups

Various US-based civil liberty or pressure groups seek have weighed in on encryption issues with the overwhelming majority coming out in favour of strong-encryption. This is sometimes connected to the commercial pressures faced by technology firms (as outlined above). Internet Association is a trade association that represents global internet companies on matters of public policy.[326] Its membership comprises a variety of the private actors that are heavily involved in US encryption disputes including Google and Facebook.[327] The association has developed clear positions on issues including privacy,[328] government data collection,[329] and data security[330] where it represents the interests of its members. Internet Association has therefore unsurprisingly supported strong encryption. Internet Association CEO Michael Beckerman issued a statement that claimed 'weakening encryption by requiring companies to engineer vulnerabilities into their services makes us all less safe and less secure.'[331] In response to the Compliance with Court Orders Act of 2016 that sought to compel Apple to assist the FBI, Beckerman stated that the order 'will harm national security and put Americans at risk', given that 'strong encryption is vital to protecting national security, personal privacy, communications, the electric grid, hospitals, and our defense systems. Mandating the weakening of encryption will put the United States' national security and global competitiveness at risk without corresponding benefits.'[332]

[326] "We Are the Voice of the Internet Economy," Internet Association, accessed April 1, 2018, https://internetassociation.org/.
[327] "Our Members," Internet Association, accessed April 1, 2018, https://internetassociation.org/our-members/.
[328] "Privacy," accessed April 1, 2018, https://internetassociation.org/positions/privacy/.
[329] "Government Data Collection," Internet Association, accessed April 1, 2018, https://internetassociation.org/positions/law-enforcement/.
[330] "Data Security," Internet Association, accessed April 1, 2018, https://internetassociation.org/positions/data-security/.
[331] "Statement on Encryption," Internet Association, November 23, 2015, https://internetassociation.org/112315encryption/.
[332] "Statement on the Compliance with Court Orders Act of 2016," Internet Association, April 11, 2016, https://internetassociation.org/041116encryption/.

Organisations including the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Centre also advocate for strong-encryption, albeit for ideologically-motivated reasons. These organisations see encryption as an important mechanism for which to guarantee the central values they protect including privacy. Advocacy groups also actively promote tools and techniques that ensure American citizens implement encryption on both their devices and in their communication. The ACLU has recommended privacy-focused applications including Signal and Tor[333] while the EFF has published a 'Secure Messaging Scorecard' that compares communication applications based on numerous variables including whether communication data is encrypted in transit, if contact identities can be verified and if there has been a recent code audit.[334] Advocacy groups such as the ACLU and EFF have a degree of political power – both by scrutinising policy and legal proposals and in promoting the importance of strong-encryption, thereby enhancing public debate.[335]

WikiLeaks is another non-profit organisation that has been highly influential. It released the CIA Vault 7 documents, which included information on CIA efforts to access encrypted data (outlined above), that put pressure on the CIA. However, the motivations and incentive structures of WikiLeaks are unclear. The organisation's goal is 'to bring important news and information to the public' and its stories typically involve leaked documents in areas related to issues such as surveillance, corruption and abuse of power. However, suspicions about its motives have surfaced given its leaking of information in the context of the US 2016 presidential election creating suspicion that the group was either a Russian front or a witting

[333] Daniel Kahn Gillmor and Jay Stanley, "A Few Easy Steps Everyone Should Take to Protect Their Digital Privacy," ACLU, June 7, 2016, https://www.aclu.org/blog/privacy-technology/internet-privacy/few-easy-steps-everyone-should-take-protect-their-digital.
[334] "Secure Messaging Scorecard," Electronic Frontier Foundation, November 3, 2014, https://www.eff.org/node/82654.
[335] Interview with a cyber security, privacy, and encryption academic.

agent through which Russia has been able to conduct disinformation campaigns. While WikiLeaks may therefore publish on issues related to US encryption policy, there is at least the possibility that the organisation is doing it for altogether different reasons when compared to the ACLU or EFF – that is, given an anti-Western sentiment as opposed to a desire to protect civil liberties and rights guaranteed by the US constitution.

Various think tanks and advocacy groups have also examined the issue. Although too numerous to name all of these individually, think tanks cater to both their funders and political actors that engage with them. This has meant that their coverage through talks, workshops and publication has included both strong and weak-encryption arguments, as well as more neutral perspectives.[336]

Individuals can also have an impact within the US encryption assemblage. Snowden is clearly the most visible example of this – the leaking of NSA documents had two decisive impacts. First, it led to significant scrutiny and suspicion on US government actors. By revealing the ways in which the NSA has sought to access data and bypass encryption, pressure was put on these security actors to stop such practices and to become more transparent in their activities. Second, the revelations have led to Americans becoming more privacy conscious. This has led to a rise in popularity of privacy focused applications such as Signal, Tor and Proton Mail.

Media and News Outlets

Given the public nature of US encryption debates, media outlets have been highly influential in setting the agenda. News organisations including The Guardian and The Washington Post

[336] For example, see "Encryption Policy in Democratic Regimes Finding Convergent Paths and Balanced Solutions" (New York: EastWest Institute, 2018), https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf?dm_i=439P,3E9,1AF62,7Z5,1; Jack Karsten, "Alternative Perspectives on Encryption," Brookings, May 12, 2016, https://www.brookings.edu/blog/techtank/2016/05/12/alternative-perspectives-on-encryption/; "Promoting a Secure Internet,"; "Read This Before You Rail Against Encryption."

played a decisive role in breaking many of the stories involving the documents leaked by Snowden.[337] Glenn Greenwald, one of The Guardian journalists heavily involved, left the organisation to setup his own new site, The Intercept which has gone on to provide a critical lens of government surveillance and anti-encryption initiatives.[338]A variety of other news outlets have also covered encryption issues closely. Naturally a balance of opinions exists, although the majority of mainstream outlets have taken a pro-encryption stance. For example, The Wall Street Journal, The New York Times and The Boston Globe have all published either editorials or opinion pieces that support technology firms in adopting strong encryption standards.[339]

This is also reflected in TV media. Various outlets in the US have covered the issue in depth as Snowden leaked NSA documents and in the Apple-FBI encryption dispute. This has included high-profile reporting. For example, the Apple-FBI encryption dispute filled the main segment on influential political satirist John Oliver's late-night HBO show Last Week Tonight with the segment favouring Apple's stance protecting encryption.[340] Influential political satirist[341] John Oliver also made an argument for strong-encryption on his show Last Week Tonight with the

[337] This has been recognised with both newspapers winning the Pulitzer Prize for their reporting on the Snowden revelations. See, Ed Pilkington, "Guardian and Washington Post Win Pulitzer Prize for NSA Revelations" The Guardian, April, 14, 2014, https://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations.
[338] Micah Lee, "Encrypting Your Laptop Like you Mean It," The Intercept, April 27, 2015, https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/.
[339] "The Encryption Farce," The Wall Street Journal, April 25, 2016, http://www.wsj.com/articles/the-encryption-farce-1461624399; "Apple Is Right on Encryption," The Wall Street Journal, March 2, 2016, http://www.wsj.com/articles/apple-is-right-on-encryption-1456877827; Cameron F Kerry, "The Backdoor Threat to Encryption," The Boston Globe, October 1, 2015, https://www.bostonglobe.com/opinion/editorials/2015/10/01/the-backdoor-threat-encryption/xprHAyG12AAFCVvrrkE6OO/story.html; Bruce Schneier, "A 'Key' for Encryption, Even for Good Reasons, Weakens Security," The New York Times, July 15, 2016, https://www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security.
[340] Eric Geller, "'Crypto Wars' Timeline: A History of the New Encryption Debate," The Daily Dot, April 26, 2016, https://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/; Victor Luckerson, "How the 'John Oliver Effect' Is Having a Real-Life Impact," *Time*, July 10, 2015, http://time.com/3674807/john-oliver-net-neutrality-civil-forfeiture-miss-america/.
[341] ibid.

segment gaining over nine million views on YouTube and 1.2 million views on Facebook (as of February 2018).

Academic Actors

Academics have played a decisive role in US encryption and privacy debates. Many of the elite US universities have established pro-encryption and pro-privacy communities and have played a decisive role in the development of ARPANET and the internet. MIT and Berkeley University both host research initiatives that advocate the importance of strong encryption for example.[342] One interviewee who has been heavily involved in academic privacy research also explained how academics use their technical understanding of encryption to meaningfully contribute to developing protocol and formal methods analysis that is then often implemented by technology firms in their encryption protocols.[343]

Established pro-privacy or pro-encryption academics are followed widely within the cyber security community. Harvard-based Bruce Schneier has one of the most widely followed cyber security blogs.[344] Academics also engage closely with technology policy. In response to recent encryption disputes, a group of well-known and well respected security researchers jointly published a paper that made a compelling agreement for the ways that government backdoors would fundamentally weaken encryption and cyber security.[345] Academics are also consulted

[342] This is in reference to MIT's Computer Science & Artificial Intelligence Lab and Berkeley's Department of Electrical Engineering and Computer Sciences have cryptography research groups for example. See, "Cryptography and Information Security Group," MIT Computer Science & Artificial Intelligence Lab, December 5, 2017, https://crypto.eecs.berkeley.edu/; "Crypto@berkeley," The Cryptography Group, accessed March 26, 2018, https://crypto.eecs.berkeley.edu/; Interview with David Clark by the Author. June 1, 2017. Cambridge, MA.
[343] Interview with a cyber security, privacy, and encryption academic.
[344] Bruce Schneier, "Schneier on Security," Schneier on Security, accessed March 26, 2018, https://www.schneier.com/.
[345] Harold Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications."

in the policy-making process.[346] For example, Matthew Blaze, one of the leading strong-encryption advocates has testified in various subcommittees on encryption.[347] Although advocacy groups and academia might therefore lack overt political power, they nonetheless can have influence through providing expertise and scrutiny that informs political and legal processes. Blaze, for instance, had a significant impact on previous encryption debates in the US when he broke the Clipper Chip.[348] Likewise, Daniel Bernstein argued against export controls on encryption based on the first amendment[349] – although unsuccessful in winning the case, he nonetheless generated a significant amount of publicity over strong-encryption according to one interviewee heavily involved in the US digital privacy community.[350]

* * *

Having outlined the most relevant security actors involved in the US Encryption Security Assemblage, there is clearly a complex network of actors and a variety of incentive structures at play and with power and capabilities distributed across the assemblage.

Internal divergence within an actor type is a clear theme. The US Government provides the best example of this – a variety of government entities approach the encryption issue with different perspectives and motivations, making the 'US Government' an incoherent collective of competing incentives. The same is true of technology firms, which comprise strong-encryption actors (for both commercial and ideological reasons) as well as weak-encryption actors that instead profit by developing the means to access encrypted data. Such complexity

[346] Interview with a cyber security, privacy, and encryption academic.
[347] Matt Blaze, "Testimony of Dr. Matt Blaze," § US House of Representatives Committee on Government Oversight and Reform Information Technology Subcommittee Encryption Technology and Possible US Policy Responses (2015), http://www.crypto.com/papers/governmentreform-blaze2015.pdf; Blaze, Matt, "Testimony of Dr. Matt Blaze," § The Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space (1996), https://fas.org/irp/congress/1996_hr/960626_blaze_test.htm.
[348] Interview with a cyber security, privacy, and encryption academic; Brock N Meeks, "Clipping Clipper: Matt Blaze," Wired, September 1, 1994, https://www.wired.com/1994/09/clipping-clipper-matt-blaze/.
[349] Burnstein v. United States Department of Justice, No. 97–16686 (United States Court of Appeals, Ninth Circuit. May 6, 1998).
[350] Interview with a cyber security, privacy, and encryption academic.

within traditional units reinforces the importance of studying actors more specifically and in greater depth, as well as exploring inter-unit clusters when appropriate. The insight gained from such a deep dive is one of the main reasons why thinking with assemblages represents a useful way to examine the network of cyber security providers through an assemblage framework.

The vast majority of actors support either strong or weak-encryption – the US Encryption Security Assemblage is therefore more appropriately captured through two inter-unit clusters. By moving at least partially beyond the traditional units used in IR, it is possible to understand the dynamics that exist between encryption actors with a more coherent and nuanced lens, and crucially one that can articulate practical security concerns.

Assemblage Dynamics: unstable and contentious disputes

The two key traits of the US Encryption Security Assemblage Configuration outlined above were the variety of incentive structures and the broad distribution of power across actors on both sides of the encryption debate. As this Assemblage Dynamic section will show, these factors have had a significant bearing in developing highly fragmented, unstable and disharmonious assemblage dynamics.

Internal Workings of the US Encryption Security Assemblage

The Assemblage Configuration has a clear bearing on the internal dynamics within the US Encryption Assemblage. The number of actors, alongside the variety of incentive structures and the diffusion of power across various actors are crucial variables that have led to both disharmony and fragmentation. There is a significant lack of fusion with the majority of actors ontologically distinct and possessing their own agency and set of motivations. The practices within the US Encryption Assemblage drive wedges between actors. Tensions exist on three accounts within the assemblage: conflict between strong and weak-encryption clusters, conflict

within each of these inter-unit clusters and tensions within traditional units (most notable when examining the dynamics between US Government actors).

The conflict between strong and weak-encryption clusters represent the most significant source of tension and disharmony. Literature associated with critical security studies has established that the notion of security is a social construction and therefore relative term that holds different meanings for different actors and groups[351] – a phenomena clearly observed in this case study. Encrypted data is either accessible or not. The alternative visions of security within the US Encryption Assemblage pursued by strong and weak-encryption actors are mutually exclusive – the majority of the multiple securities observed are therefore also clashing securities. Strong and weak-encryption actors have largely been unable to cooperate on the issue or reach a compromise. Intelligence and law enforcement actors pursue more conventional visions of security and seek to protect the US from foreign threats, terrorism and serious organised crime. Accessing encrypted data is perceived as important in these contexts in order to obtain relevant intelligence or evidence. Technology firms and other actors including academia and advocacy groups, by contrast, pursue alternative visions of security including economic security and societal forms of security (most notably privacy).

This disharmony is observed through various confrontational practices. From a technical perspective, both strong and weak-encryption actors are in a persistent skirmish over data access. Central government actors including the President's office and Congress have been either unable or unwilling to introduce legislation that would significantly change the situation in favour of weak-encryption actors. Yet, weak-encryption actors have not been prevented from trying to access encrypted data themselves, and the FBI, for instance, is constantly exploring new ways to access encrypted data, through developing exploits and processes that undermine

[351] Gallie, "Essentially Contested Concepts," 6-8.

data security. Weak-encryption actors either develop such capabilities internally or through outsourcing to third parties[352] (indeed, outsourcing is one of the rare practices where cooperation between different security actors occurs). Strong-encryption actors, by contrast, constantly seek to keep encrypted data inaccessible from weak-encryption actors. As strong-encryption actors discover the means in which weak-encryption actors have accessed data, they will respond directly – for example, through patching a vulnerability used to access encrypted data. At a political level, both sides have also engaged in lobbying, attempting to push their views and agenda forward towards actors with significant political power including Congress and the Executive Branch.[353] Weak-encryption actors have also challenged strong-encryption policies on legal grounds: using court orders, and attempting to pass legislation in an effort to compel weak-encryption actors against their will. Accompanying political and legal confrontations is a highly public debate of ideas. Press statements, media appearances and written publications from both strong and weak-encryption actors have sought to dismiss the other side's arguments and to win over public opinion.

There is a clear securitisation process in place, stemming from governmental weak-encryption actors. Securitisation refers to a process whereby the existence of a threat legitimises the use of certain measures (often from the perspective of government actors).[354] In the context of this case study, various threats are invoked by weak-encryption actors in an attempt to justify restrictions on encryption. FBI Director Christopher Wray claimed that encryption causes problems 'across the board – human trafficking, counterterrorism, counterintelligence, gangs,

[352] Carman, "An Israeli Company Is Reportedly Helping the FBI Crack the San Bernardino iPhone,"; Alina Selyukh, "The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?"
[353] Lynch, "Newly Released Documents Detail FBI's Plan to Expand Federal Surveillance Laws,"; Flyverbom, "Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations," 122; "Lobbying Spending Database - Facebook Inc,"; Solon and Siddiqui, "Forget Wall Street – Silicon Valley Is the New Political Power in Washington."
[354] Barry Buzan, Ole Wæver, and Jaap de Wilder, *Security: A New Framework of Analysis* (Boulder, CO: Lynne Rienner, 1998).

organized crime, child exploitation, and cyber.'[355] Likewise, terrorist incidents will often immediately precede arguments for weak-encryption. For instance, the then FBI Director James Comey claimed that 'the use of encryption is at the center of terrorist trade craft' shortly after the 2015 Paris terrorist attack.[356] The then CIA Director John Brennan also cited the Paris attack to argue that US surveillance policy is too restrictive.[357] These statements were made despite the fact that the terrorists in question used burner phones, rather than encryption to evade detection.[358] These forms of 'speech acts' are used to justify policy positions[359] – in this case, greater restrictions on encryption. Court orders and proposed legislation have subsequently sought to compel strong-encryption actors against their will. Yet, governmental weak-encryption actors have often lacked the necessary power and capability to successfully securitise the issue of encryption to the extent that they would have hoped. Indeed, encryption represents one instance where security-relevant government actors (such as the intelligence and law enforcement community) are having their intentions and visions of security fundamentally questioned. Non-governmental actors have risen to a level of political agency where they are actively challenging the intelligence and law enforcement communities' vision of security.[360]

The prevailing source of disharmony within the US Encryption Assemblage stems from the disputes between strong and weak-encryption clusters, yet neither of these inter-unit clusters

[355] Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation."
[356] Evan Perez and Shimon Prokupecz, "Paris Attackers Likely Used Encrypted Apps, Officials Say," CNN, December 17, 2015, https://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/index.html.
[357] John Hudson, "Citing Paris Attack, CIA Director Criticizes Surveillance Reform Efforts," Foreign Policy, November 16, 2015, https://foreignpolicy.com/2015/11/16/citing-paris-attack-cia-director-criticizes-surveillance-reform-efforts/.
[358] Glyn Moody, "Paris Terrorists Used Burner Phones, Not Encryption, to Evade Detection," Ars Technica, March 21, 2016, https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/; Trevor Timm, "Paris Is Being Used to Justify Agendas That Had Nothing to Do with the Attack," The Guardian, November 20, 2015, https://www.theguardian.com/commentisfree/2015/nov/20/paris-attacks-political-agenda-immigration-encryption-surveillence.
[359] Buzan, Wæver, and de Wilder, *Security: A New Framework of Analysis*.
[360] Indeed, the role of private sector norm development has been chronically under analysed yet is a hugely important phenomenon in cyber security. For further depth on this issue, see, Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs," *Journal of Cyber Policy*, (April 27, 2018): 1–16.

are themselves particularly hybrid. Indeed, within each of these coalitions of sorts, there are clear instances of fragmentation and even tension.

Advocates of weak-encryption are often unwilling to work together. The various actors that form the US intelligence community cluster nonetheless remain distinct entities. This should not necessarily be a surprise with the US intelligence and law enforcement community having a record of not cooperating properly – indeed, it has been argued that the lack of coordination between these agencies was one of the core reasons why 9/11 was not prevented.[361] The lack of cooperation and divergent incentive structures are clearly observed in the US Encryption Assemblage – most clearly through the differences in intelligence-gathering and evidence-producing missions. Publicly available evidence suggests that the NSA has the most sophisticated capability from a material power perspective – both the Snowden and Shadow Broker[362] leaked documents and toolkits confirm this much. Out of all the weak-encryption actors, the NSA is therefore most likely to be able to access encrypted data. Despite its clear technical capability, the NSA was notably absent from the FBI's encryption dispute with Apple given the diverging incentive structures of the two agencies.[363] As an intelligence agency, the NSA does not need to produce conclusive proof. This means that breaking encryption is one of a number of ways that the NSA can gather intelligence – it might also use other techniques including analysing metadata or breaking into related systems (such as a nearby CCTV camera

[361] James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (New York: Anchor, 2009); Barbara A Grewe, "Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations" (Washington, DC: Commission on Terrorist Attacks Upon the United States, August 20, 2004); Bruce Schneier, "FBI/CIA/NSA Information Sharing Before 9/11," Schneier on Security, November 11 2009, https://www.schneier.com/blog/archives/2009/11/fbiciansa_infor.html.

[362] The Shadow Brokers is an online pseudonym that has released stolen NSA secrets online. See, TheShadowBrokers, "REPOST: TheShadowBrokers Message#1 - August 2016," Steemit, June 30, 2017, https://steemit.com/shadowbrokers/@theshadowbrokers/repost-theshadowbrokers-message-1-august-2016; Bruce Schneier, "Who Are the Shadow Brokers?," *The Atlantic*, May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

[363] Russell Brandom, "Why the NSA Is Staying out of Apple's Fight with the FBI," The Verge, March 9, 2016, https://www.theverge.com/2016/3/9/11186868/apple-fbi-nsa-encryption-exploit-hack; Jenna McLaughlin, "NSA Is Mysteriously Absent From FBI-Apple Fight," The Intercept, March 3, 2016, https://theintercept.com/2016/03/03/nsa-is-mysteriously-absent-from-fbi-apple-fight/.

of an adversary's location). The NSA also favours secrecy, thereby decreasing the chances that vendors will find out about their techniques and thereby enabling the NSA to make the most of their capability.[364] The FBI, by contrast, is a law-enforcement agency and therefore seeks to produce evidence that ends up in open courts.[365] This explains why the FBI did not exhaust all possible technical solutions to unlock the iPhone connected to the San Bernardino shooting before seeking a court order to compel Apple's assistance[366] given that establishing a legal precedent is more in line with their interests (indeed, on this point, conflict and dispute with strong-encryption actors is openly in the FBI's interests if it enables them to gain access to encrypted data in a more structured manner). By assisting the FBI, the NSA would effectively be degrading and undermining its own capability, making its own mission demonstrably more challenging.[367] Further, as a foreign intelligence agency the NSA is motivated to access the data of foreign targets. Here, there are divergences in the technology used between the US domestic demographic that the FBI is interested in and the foreign actors that the NSA targets. The NSA's incentive structures therefore encourage it to use its capabilities to access different forms of data when compared to the FBI. While the NSA may have the most impressive material capability to break into devices and communication services used within the US at a theoretical level, it has not directed most of its resources here at a practical level.

Strong-encryption actors seek to secure data for altogether different reasons. Encryption debates have often been characterised as a debate between privacy and security,[368] yet such a

[364] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*.
[365] Brandom, "Why the NSA Is Staying out of Apple's Fight with the FBI,"; Jenna McLaughlin, "NSA Is Mysteriously Absent From FBI-Apple Fight," The Intercept, March 3, 2016, https://theintercept.com/2016/03/03/nsa-is-mysteriously-absent-from-fbi-apple-fight/.
[366] "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation" (Office of the Inspector General U.S. Department of Justice, March 2018).
[367] Brandom, "Why the NSA Is Staying out of Apple's Fight with the FBI,"; McLaughlin, "NSA Is Mysteriously Absent From FBI-Apple Fight."
[368] Mary Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era" (Pew Research Center, November 12, 2014).

framing misrepresents the motivations of various strong-encryption advocates. Crucially, while many strong-encryption technology firms have resisted the attempts of intelligence and law enforcement actors to access their users' data, they are not necessarily doing so wholly out of principle. Many of the services run by strong-encryption actors, such as Facebook and Google services appear to be free but users are required to share their data.[369] Using and commercialising user data is therefore central to the business model of many actors in the profit-motivated technology firm cluster. Advertising accounted for 87 and 98 percent of Google and Facebook's revenue respectively.[370] These technology firms typically make money on a 'cost-per-click' basis meaning that they get paid as and when users click on adverts – the effectiveness of their advertisements is therefore crucial. Technology firms have therefore targeted their advertisements to specific demographics and this has required these firms to collect and use personal data to build up a profile of a particular user in order to understand their tastes and interests.[371] It would also appear that many strong-encryption technology firms are not wholly opposed to government surveillance when it suits their interests. For example, many actors within the profit-driven technology firm cluster were largely absent from a debate in the US related to the renewal of the Foreign Intelligence Surveillance Act as blocking the renewal could jeopardise the trans-Atlantic data transfer pact known as the 'Privacy Shield' that underpins billions of dollars in trade in digital services[372] and enables interoperability between European and US data protection standards.[373] By challenging US surveillance

[369] "How to Tame the Tech Titans," The Economist, January 18, 2018, https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame.
[370] Davey Alba, "Google and Facebook Still Reign Over Digital Advertising," Wired, July 29, 2017, https://www.wired.com/story/google-facebook-online-ad-kings/.
[371] ibid.
[372] Dustin Volz, "Silicon Valley Mostly Quiet in Internet Surveillance Debate in Congress," Reuters, July 18, 2017, https://uk.reuters.com/article/us-usa-intelligence/silicon-valley-mostly-quiet-in-internet-surveillance-debate-in-congress-idUKKBN1A32B3.
[373] "Privacy Shield Overview," Privacy Shield, accessed April 1, 2018, https://www.privacyshield.gov/Program-Overview.

practices, US-based technology firms would risk European regulators determining that US standards were not at a sufficient level to correlate with European standards.[374]

The motivations and actions of profit-driven strong-encryption actors contrasts starkly with ideologically-motivated technology firms. Messaging applications including Telegram and Signal are ran on a not-for-profit basis and have developed encrypted communication applications on ideological grounds. Although both profit and non-profit strong-encryption actors work together (Skype, Facebook and WhatsApp have all implemented Signals' secure messenger encryption protocol for example), there is nonetheless tension between these actors. Telegram has clearly distanced itself from profit-driven technology firms despite their mutual support for strong-encryption, arguing that 'big internet companies like Facebook or Google have effectively hijacked the privacy discourse in the recent years' and argued that many of their privacy features are superficial, allowing you to hide information from those around you, rather than protecting personal data and private conversation from third parties – whether government officials, marketers or advertisers.[375] The disputes between strong-encryption actors is further observed through the activities of advocacy groups. While actors including the EFF and ACLU have publicly sided with profit-driven technology firms on encryption debates, they have simultaneously publicly criticised the privacy policy of these actors. Both the EFF and ACLU have published guidance and criticism on Facebook's privacy policy for example.[376]

The disputes within each inter-unit clusters also reveal the tensions that exist within the traditional units used in IR. Internal security disputes are most clearly seen between US Government actors where a number of securities, interests and objectives exist, ranging from

[374] Volz, "Silicon Valley Mostly Quiet in Internet Surveillance Debate in Congress."
[375] "Telegram FAQ," Telegram, accessed June 20, 2018, https://telegram.org/faq#q-what-are-your-thoughts-on-internet-privacy.
[376] Kurt Opsahl, "Facebook's Eroding Privacy Policy: A Timeline," Electronic Frontier Foundation, April 28, 2010, https://www.eff.org/deeplinks/2010/04/facebook-timeline; "Facebook: A Privacy Guide," ACLU, accessed April 1, 2018, https://www.aclu.org/other/facebook-privacy-guide.

intelligence and law enforcement (as addressed above) to economic growth, and enabling dissidence abroad.[377] The weak-encryption arguments stemming from the US law enforcement community do not correlate with the State Department's desire to promote a free, open and secure internet for example. A variety of views exist within the intelligence, law enforcement and security community on the issue of encryption – often with active disagreement between different entities. There are also internal tensions for various actors – the NSA and Department for Homeland Security for example have a dual mission of intelligence gathering and cyber security with these missions often contradicting one another.[378] Despite the Executive's relatively neutral and uninvolved stance on the issue, they have nonetheless introduced the VEP[379] that constrains the actions of intelligence and law enforcement actors seeking to break into systems, requiring them to justify why the vulnerabilities they use should not instead be disclosed to technology vendors, thereby enabling them to be patched.[380]

Turning to corporations, while many technology firms seek to develop encryption that prevents government access, the thriving surveillance-ware market[381] provides a financial incentive for firms to find the means to access encrypted data (either through breaking encryption standards

[377] Joseph Menn and Dustin Volz, "Apple Case Exposes Ongoing Government Rift over Encryption Policy," Reuters, March 8, 2016, https://www.reuters.com/article/us-apple-encryption-schism-insight/apple-case-exposes-ongoing-government-rift-over-encryption-policy-idUSKCN0W70U5.
[378] Collier and Silomon, "Security Dichotomies in Cyber Security."
[379] Rob Joyce, "Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do," The White House, November 15, 2017, https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/; "Vulnerabilities Equities Policy and Process for the United States Government" (Washington DC: The White House, November 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; "Fact Sheet: Vulnerabilities Equities Process" (Washington, DC: White House, November 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20White%20House%20Fact%20Sheet%20on%20VEP%20-%20FINAL%2011152017.PDF.
[380] For further context over the tensions and debates related to the VEP, see Dave Aitel and Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," Lawfare, August 18, 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong; Benjamin Wittes, *The Lawfare Podcast: Dave Aitel and Matt Tait on How "Everything You Know About the Vulnerability Equities Process Is Wrong,"* The Lawfare Podcast, August 27, 2016. https://www.lawfareblog.com/lawfare-podcast-dave-aitel-and-matt-tait-how-everything-you-know-about-vulnerability-equities.
[381] Cox, "Government Malware Company 'Grey Heron' Advertises Signal,"; Cox, "Documents Prove Local Cops Have Bought Cheap iPhone Cracking Tech,"; Cox and Franceschi-Bicchierai, "How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of."

or more commonly through compromising devices). Such disharmony within actor types reinforces a central argument of this thesis regarding the multiple agencies, agendas and motivations that exist within both the government and private sector. While this is also the case in other instances outside of cyber security (and by no means a novel phenomenon), it nonetheless reinforces the constructed, and fluid nature of the concepts used to capture the international system.

Evolution: technical, political and legal instability

The US Encryption Assemblage is in a constant state of evolution that is highly unstable. Two factors previously examined explain this evolutionary process: the fragmentation of power across different actors and the variety of incentive structures that exist. Combined, they mean that the various pockets of capability are often moving in different (and often contradictory) directions. There is no single actor, nor a coalition of actors, on either side of the debate, that possess the capability to achieve and sustain a decisive level of dominance in either protecting or accessing encrypted data. There is no reason to believe that such a reality will change going forward. In the absence of dominance, it is therefore likely that the US Encryption Assemblage will continue to be characterised by persistent contestation as both strong and weak-encryption actors continue to compete.

The previous discussion on power did suggest that strong-encryption actors enjoy certain advantages at present from a technical perspective (such as the low barriers to entry in developing encryption standards, the relative ease in patching systems as opposed to finding new vulnerabilities and exploits, etc.). The historical backdrop from previous encryption disputes would also appear to confirm this: while US Government actors have tried to limit the proliferation and use of encryption during the first ‘Crypto Wars’, ultimately the technology

was implemented at scale.[382] Yet, both the historic and current advantages enjoyed by strong-encryption actors is highly precarious; any advantage strong-encryption actors do possess does not equate to dominance.

Instability is reflected within a variety of contexts in the US Encryption Security Assemblage. From a technological perspective, the battle between strong and weak-encryption actors over the protection and access of encrypted data is iterative. There is a constant back-and-forth process: weak-encryption actors find a means to access encrypted data; strong-encryption actors attempt to deny such access through updating and modifying their systems as and when they discover the vulnerabilities that have been exploited by weak-encryption actors that have gained accessed; weak-encryption actors then explore alternative means of access and the process repeats. This means that sometimes strong-encryption actors will be ahead while at other times weak-encryption actors will be. This can be observed in practice: while in late 2017, it was claimed that the FBI was unable to access over 7,500 during the year (although as previously stated, the number was in fact under 2,000),[383] by February 2018, it had emerged that the agency was able to access a large variety of phones through tools purchased from private surveillance-ware producers.[384] Crucially, the changes or ability to access data (or not) change very fast. It is true that as time goes on, it will become more difficult for weak-encryption actors to access a particular form of hardware or software that stores encrypted data – as more of the vulnerabilities and means of access are patched. Yet, technology is dynamic. Device manufacturers, software producers and communication applications are in a constant

[382] Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s,"; Thomas Rid, *Rise of the Machines: The Lost History of Cybernetics* (London, UK: Scribe, 2016) pp.246-293.
[383] Ong, "The FBI inflated the number of encrypted phones linked to crime,"; interview with a cyber security journalist with the author. London, UK. May 24, 2018; Sarah N Lynch and Brendan Pierson, "U.S. Attorney General Says Tech Companies Should Help Access Encrypted Evidence."
[384] Joseph Cox, "Military, FBI, and ICE Are Customers of Controversial 'Stalkerware,'" Motherboard, February 23, 2018, https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware.

process of building and releasing newer versions of their product that offer more features. This means that the attack surface is constantly shifting and thus open to altogether new vulnerabilities and means of access for weak-encryption actors. This back-and-forth nature of encryption disputes is therefore likely to sustain, given the inherently dynamic characteristics of technology.

The instability of the US Encryption Assemblage also extends beyond technical measures with encryption disputes also unresolved from a legal perspective with no clear precedent on the issue established. The two most high-profile legal cases that have sought to compel Apple to assist law enforcement in providing access to its devices in New York and California have both been dropped.[385] The various federal cases that have been completed have led to mixed results with some ruling more favourably with law enforcement and some with technology firms.[386]

[385] Joel Rubin, James Queally, and Paresh Dave, "FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle With Apple, For Now,"; Danny Yadron, "San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance," The Guardian, March 29, 2016, http://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone; Russel Brandom, "With its Retreat in New York, the FBI has Lost the Encryption Fight," The Verge, April 25, 2016, https://www.theverge.com/2016/4/25/11501992/fbi-apple-new-york-case-unlock-iphone-lost.

[386]Attempts to invoke the All Writs Act to compel Apple to assist in decrypting devices has been met with mixed results at the state level. A New York federal magistrate judge denied the US Government's request that Apple should extract data from an iPhone related to a drug case in New York in 2016. A Massachusetts magistrate judge also ordered Apple to provide 'reasonable technical assistance' to the FBI in a Boston gang case in 2016. Crucially, however, while Apple was required to assist in extracting data from the phone, the ruling did not include any obligation to decrypt data. There have also been mixed results in relation to key disclosure work – i.e. Compelling criminals to reveal their encryption key or device password. While judges have ruled that criminal suspects are required to assist law enforcement in this matter, judges have also ruled that doing so would violate the Fifth Amendment right against self-incrimination in other cases. See, James Orenstein, In Re Order Requring Apple, INC. to Assist in the Execution of a Search Warrant Issued by this Court (United States District Court Eastern District of New York February 29, 2016); In re Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mJ-91, 2009 WL 424718 (United States District Court for the District of Vermont February 19, 2009); United States of America v. Ramona Camelia Fricosu, a.k.a. Ramona Smith, No. 841 F.Supp.2d 1232 (United States District Court for the District of Colorado January 23, 2012); United States of America v. Thomos J. Kirschner, No. 823 F. Supp. 2d 665 (United States District Court for the Eastern District of Michigan March 30, 2010); "Appeals Court Upholds Constitutional Right Against Forced Decryption," Electronic Frontier Foundation, February 24, 2012, https://www.eff.org/press/releases/appeals-court-upholds-constitutional-right-against-forced-decryption; Katie Benner and Joseph Goldstein, "Apple Wins Ruling in New York iPhone Hacking Order," The New York Times, February 29, 2016, https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.htm; Alison Bauter, "FBI vs. Apple: Massachusetts Judge Sided with Feds in Gang Case, Records Show," Boston Patch, April 8, 2016, https://patch.com/massachusetts/boston/judge-sides-fbi-against-apple-boston-gang-case-0; Cyrus Farivar, "Massachusetts High Court Orders Suspect to Decrypt His Computers," Ars Technica, June 26, 2014, https://arstechnica.com/tech-policy/2014/06/massachusetts-high-court-orders-suspect-to-decrypt-his-computers/.

Crucially, however, in none of the cases so far have technology firms been compelled against their will to assist law enforcement in accessing encrypted data. This suggests that strong-encryption actors have an advantage at present from a legal perspective. Yet, such an advantage is not necessarily stable going forward. With the issue unresolved, there are likely to be further court battles – especially when law enforcement actors are unable to access encrypted data through exploiting vulnerabilities and other technical means. While there is not a legal precedent that compels technology firms to assist law enforcement in accessing encrypted data, there is also no legal precedent that effectively rules out such a possibility, or prevents law enforcement actors from attempting to access encrypted data themselves (either independently or via third parties).

Even if the legal battles between law enforcement and technology firms have not been decisive, this might have still helped either side of the debate if it led to political developments: legislation that either compels technology firms to assist law enforcement or bans such arrangements for example. Yet, the issue of encryption is also unresolved from a political perspective and currently sits at a stalemate[387] in a form of political gridlock. Initiatives and legislative proposals have gone in both directions: while The Compliance with Court Orders Act of 2016 that demanded assistance from tech firms was dropped, The Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016 that would prevent US states from regulating or controlling the kind of encryption that technology firms are able to use was also introduced in 2016 yet still has not been decided upon. Although Democrats have recently been more sympathetic and supportive of strong-encryption, both Republican and Democrats have yet to really develop coherent positions on the issue.[388] The Executive Branch of the US Government has also stalled in acting on the issue of encryption and faces a difficult

[387] Interview with Adam Segal.
[388] Kaveh Waddell, "Is Digital Privacy Becoming a Partisan Issue?," *The Atlantic*, March 7, 2016, https://www.theatlantic.com/technology/archive/2016/03/is-digital-privacy-becoming-a-partisan-issue/472449/.

balancing act given the variety of government entities and their clashing agendas on the issue. It would therefore appear that the political advantage is with strong-encryption actors given the lack of decisive initiatives that would prevent their ability to keep encrypted data inaccessible. Again, however, such an advantage is precarious. Trump's campaign rhetoric in favour of weak-encryption could turn into a concrete legislative proposal for example. The political climate is also highly dependent on public opinion.

Here, the public debate also sits finely balanced and thus largely unresolved. As discussed previously, opinion polls on the issue of encryption are indecisive, with some indicating the majority of respondents support strong-encryption while other suggest greater support for weak-encryption. Opinion polls also show that public opinion can change quickly over time on the issue. In this regard, a variety of factors could possibly influence public opinion. If memories of the Snowden leaks increased distrust in government actors on data-related issues, it may be that support for strong-encryption dissolves over time as memory of the Snowden story begin to fade. Arguments for weak-encryption are often made in the aftermath of terrorist incidents, which might also change public opinion.[389] Likewise, recent mismanagement within technology firms in the context of failing to prevent various disinformation initiatives in the US might lead to a greater public distrust in technology firms, many of which are strong-encryption actors, that might also change the balance.[390] Crucially, while it is difficult, if not impossible, to forecast shifts in public opinion, it is at least clear that public opinion could go

[389] Yadron, Barr, and Wakabayashi, "Paris Attacks Fan Encryption Debate,"; Krebs, "Paris Terror Attacks Stoke Encryption Debate."

[390] For example, both Twitter and Facebook have been criticised for their roles in disinformation campaigns and through manipulating users via advertisements. See, Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," The Guardian, March 17, 2018, http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; Thomas Rid, "Why Twitter Is the Best Social Media Platform for Disinformation," November 1, 2017, https://motherboard.vice.com/en_us/article/bj7vam/why-twitter-is-the-best-social-media-platform-for-disinformation.

in various directions, depending on both external circumstances and shifts in public mood over time.

Example One: The Snowden Fallout

In May 2013, Snowden was granted leave by his NSA supervisor for two weeks, on the basis that he needed to receive treatment for epilepsy – a condition he had suffered from since a series of seizures in 2012. Packing his bags, he told his partner that he had to be away for a few weeks, elusive with details – a common occurrence for someone working in intelligence.[391] Snowden was in fact on his way to Hong Kong, having previously established contact with the journalists Barton Gellman and Glenn Greenwald from the Washington Post and The Guardian respectively, as well as documentary filmmaker Laura Portrious.[392] He had with him approximately 60GB of sensitive NSA documents. Over the next few days, he helped journalists make sense of the files in a room in the Mira Hotel.[393] Shortly after, stories began to break with the first headlines appearing in the Guardian on the 6th June 2013[394] and the Washington Post on the 7th June 2013.[395] Stories emanating from the documents continued to appear, covering a range of issues related to the NSA's intelligence gathering programmes.

The public backlash to the Snowden disclosures was significant, provoking a range of debates on the role of government intelligence collection in the digital era and developing a more

[391] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations," The Guardian, June 11, 2013, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
[392] Laura Poitras, *Citizenfour* (Praxis Films, 2014).
[393] Tom Phillips, "Edward Snowden: Hong Kong Hotel Hideaway of the NSA Whistleblower," The Telegraph, June 10, 2013, https://www.telegraph.co.uk/news/worldnews/asia/hongkong/10110927/Edward-Snowden-Hong-Kong-hotel-hideaway-of-the-NSA-whistleblower.html.
[394] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[395] Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," The Washington Post, June 7, 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

digital-privacy conscious US public[396] that increasingly questioned the role and complicity of many of the profit-motivated technology firms mentioned in this case study. Technology firms recognised a backlash against their role in cooperating with the US intelligence community though the NSA PRISM programme – where the data of users held by major internet services including Gmail, Facebook and Outlook was passed on to US Government actors.[397] The PRISM programme, as previously discussed, involved the NSA mining data from these firms directly.[398]

The consequences for profit-driven technology firms were severe in a climate of increased mistrust. A report published by The Information Technology & Innovation Foundation estimated that the US cloud computing industry stood to lose $22 to $35 billion between 2013 to 2016[399] while a paper by two Microsoft employees estimated that the Snowden leaks decreased the growth rate of revenues of US providers by 11% from the third quarter of 2013 to the fourth quarter of 2014 and would cost the US cloud industry at least $18 billion.[400] The financial filings from large technology firms also suggest negative implications: the financial fillings from IBM and Cisco reveal that the two businesses' sales have dropped by more than $1.7 billion year-on-year in the important Asia-Pacific region.[401] Having relied on American undersea cables for decades, Brazil and the EU decided to build their own cables between Brail and Portugal, awarding the contracts to Brazilian and Spanish companies.[402] Brazil also

[396] Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era."
[397] "PRISM / US-984XN Overview, or The SIGAD Used Most in NSA Reporting Overview,"; Sottek and Kopfstein. "Everything You Need to Know About PRISM."
[398] "PRISM / US-984XN Overview, or The SIGAD Used Most in NSA Reporting Overview."
[399] Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computin Industry?" (Washington, DC: Information Technology & Innovation Foundation, August 5, 2013).
[400] Hyojin Song and Simon Wilkie, "The Price of Privacy in the Cloud: The Economic Consequences of Mr. Snowden," February 2017, https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf.
[401] Mikkel Stern-Peltz and Jim Armitage, "IT Firms Lose Billions After NSA Scandal Exposed by Whistleblower Edward Snowden," The Independent, December 29, 2013, https://www.independent.co.uk/life-style/gadgets-and-tech/news/it-firms-lose-billions-after-nsa-scandal-exposed-by-whistleblower-edward-snowden-9028599.html.
[402] Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," The New York Times, March 21, 2014. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

announced plans to abandon Microsoft Outlook for its own email system using Brazilian data centres[403] and cancelled plans to confirm a $4 billion defence contract with US-based aerospace firm Boeing.[404] Many US-based technology firms also enjoy global scale and with often over sixty percent of their customers based abroad, these firms recognise that the perception that they cooperate with the US intelligence community is likely to harm their global reputation.[405]

US-based technology firms have therefore been eager to publicly distance themselves from US Government actors, recognising that the perception of a close relationship threatens both their reputation and profitability. One interviewee who formerly worked as a lawyer for the NSA even suggested ideas developed by technology firms that might help the US Government in relation to its data access requirements, whilst also keeping user data secure, have been intentionally suppressed by technology firms as they recognise the dangers of appearing to work with the US intelligence community.[406] Implementing strong-encryption has proved a highly effective and popular means for technology firms to publicly distance themselves, providing customers with more robust guarantees that their data is out of the reach for US intelligence agencies. Most large technology firms have implemented both end-to-end encryption on communication applications and introduced on-device encryption as something straightforward to implement.[407] The majority of phones, tablets and laptops are now encrypted by default with users unencrypting their devices as they unlock them with a passcode or thumbprint.[408] Alongside these changes across profit-motivated technology firms, privacy

[403] ibid.
[404] Brian Winter, "Insight: How U.S. Spying Cost Boeing Multibillion-Dollar Jet Contract," Reuters, December 20, 2013. https://www.reuters.com/article/us-boeing-brazil-insight/insight-how-u-s-spying-cost-boeing-multibillion-dollar-jet-contract-idUSBRE9BJ10P20131220.
[405] Alex Grigsby and Adam Segal, "Silicon Valley and Washington Can Be Friends If They Take These Steps," Fortune, February 2, 2017, http://fortune.com/2017/02/02/silicon-valley-washington-relationship-tech-donald-trump-encryption/.
[406] Interview with a former National Security Agency lawyer.
[407] Barrett, "The Year Encryption Won,"; O'Neill, "Android 7 Boasts New Encryption Features as the Crypto War Soldiers On," The Daily Dot, August 24, 2016, https://www.dailydot.com/layer8/android-nougat-encryption/.
[408] ibid.

focused ideologically-motivate technology firms grew in prominence – applications including Telegram and Signal were released and became increasingly popular.

Encrypted messaging applications and hard drives were therefore no longer used by just security specialists and privacy advocates but now rolled out at scale and by default. Even Americans apathetic to encryption issues therefore found their devices and applications reflecting a strong-encryption posture. While the initial backlash was therefore against US Government actors, the move provoked a response from the US intelligence and law enforcement community – a process reflected most clearly through a dispute between Apple and the FBI.

Example Two: Apple vs FBI

On the 2nd December 2015, fourteen people were killed in a mass shooting at a conference area where the San Bernardino County Department of Public Health was holding a social event.[409] The shooting was carried out by Syed Rizwan Farook, an inspector with the department, and his wife Tashfeen Malik.[410] It is widely believed that the shooting was provoked by a conversation between Farook and Malik, who were Muslims, and Nicholas Thalasinos, a colleague of Farook who was a Messianic Jew and took issue with Islam.[411] The incident was quickly treated as a terrorist incident by both mainstream journalists and the FBI (who led the investigation).[412] Amongst the evidence for the FBI to review, was one item that would rekindle

[409] "At Least 14 Dead in California Shooting," BBC News, December 3, 2015, https://www.bbc.com/news/world-us-canada-34987697.
[410] "San Bernardino Shooting: What We Know So Far," BBC News, December 11, 2015, https://www.bbc.com/news/world-us-canada-34993344.
[411] Yvette Cabrera, Rory Carroll, and Tom Dart, "San Bernardino Shooting Victim 'Had Argued with Killer About Islam,'" The Guardian, December 5, 2015, http://www.theguardian.com/us-news/2015/dec/05/san-bernardino-victim-had-argued-with-shooter-about-islam.
[412] "Terrorism," Federal Bureau of Investigation, accessed July 17, 2018, https://www.fbi.gov/investigate/terrorism; "San Bernardino Terror Attack: Police Describe Gun Battle with Terrorist Couple," Fox News, May 26, 2017, http://www.foxnews.com/us/2017/05/26/san-bernardino-terror-

longstanding privacy disputes: Farook's encrypted iPhone that had been found in a trash bin near the attackers' home.[413]

The FBI understandably sought to access the data stored on the phones as part of their investigation. The sophistication of encryption on Apple devices meant that the FBI was unable to obtain the phone data on their own and so the US Attorney Office issued a court order, seeking to compel Apple to assist the FBI in building a backdoor that could be used to bypass the encryption on the Farook's iPhone.[414]

Having distanced themselves from the US Government following the release of the Snowden documents,[415] Apple's resolve now faced its most stern and public test. Apple proceeded to contest the Attorney Office's request with CEO Tim Cook publishing a message to Apple customers on the Apple website that vowed to fight the court order arguing that the outcome 'has implications far beyond the legal case at hand.'[416] Cook suggested that there is 'no precedent for an American company being forced to expose its customers to a greater risk of attack' and that there would be no way to convincingly guarantee a backdoor would be used only in limited situations once it was created. Cook concluded that the demand 'would undermine the very freedoms and liberty our government is meant to protect.'[417] With these issues affecting technology firms at large, other senior leaders then publicly sided with Apple:

attack-terrorists-were-shot-up-to-27-times-during-gun-battle-with-police.html; "San Bernardino Shooting: What We Know So Far."
[413] ibid.
[414] Eileen M Decker et al., In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203.
[415] David E. Sanger and Brian X. Chen, "Signalling Post-Snowden Era, New iPhone Locks Out N.S.A.," The New York Times, September 26, 2014, https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.
[416] Cook, "A Message to Our Customers."
[417] ibid.

both Facebook and Twitter CEOs, Mark Zuckerburg and Jack Dorsey declared their support for Apple.[418]

The disagreement led to legal and public disputes between Apple and the FBI. A court hearing date was set for March 22 2016.[419] San Bernardino County District Attorney Michael Ramos filed a brief that bizarrely claimed that the iPhone may contain evidence of a 'lying dormant cyber pathogen that endangers San Bernardino County's infrastructure'[420] while the then FBI Director James Comey claimed that the recalcitrant stance taken by technology firms over the issue of encryption was not a technical issue related to security but a business decision and that the outcome of the legal dispute would set a precedent for future encryption disputes with encryption currently 'getting in the way of our ability to have court orders effective to gathering information we need in our most important work.'[421]

One day before the court hearing was due to take place, the FBI withdrew the court order, with the Justice Department then confirming that it had found a way to unlock the iPhone without Apple's assistance.[422]As previously mentioned, how this was achieved remains unconfirmed

[418] Jack Dorsey. Twitter post. February 18, 2016. https://twitter.com/jack/status/700457149227360256; Kurt Wagner, "Facebook, Twitter Back Apple CEO Tim Cook in Security Fight With FBI," Recode, February 18, 2016, https://www.recode.net/2016/2/18/11588026/facebook-twitter-back-apple-ceo-tim-cook-in-security-fight-with-fbi.
[419] David Ingram, "Hearing Scheduled in Apple Encryption Case for March 22," Reuters, February 19, 2016, https://www.reuters.com/article/apple-encryption-hearing/hearing-scheduled-in-apple-encryption-case-for-march-22-u-s-justice-dept-idUSL2N15Y1RF.
[420] Michael A Ramos, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (United States District Court for the Central District of California March 3, 2016).
[421] James Comey, "Senate Judiciary Committee" (2015).
[422] Yadron, "San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance."

although it is reported that the FBI paid around $1.3 million[423] to Israeli-based firm Celebrite that developed the technical tools that made it possible. [424]

As well as the fundamental debate between the law enforcement community and technology firms, the ongoing disputes over encryption highlight the instability over its security. The dispute between strong and weak-encryption actors over the protection and access of encrypted data is iterative. There is a constant back-and-forth process: weak-encryption actors find a means to access encrypted data; strong-encryption actors attempt to deny such access through updating and modifying their systems as and when they discover the way in which weak-encryption actors have accessed data; weak-encryption actors then explore alternative means of access and the process repeats. This means that sometimes strong-encryption actors will be ahead while at other times weak-encryption actors will be. This can be observed in practice: immediately after Apple discovered the FBI had gained access to Farook's iPhone, they immediately began searching for how this was achieved and later versions of the iPhone did not contain the vulnerability;[425] the FBI has since purchased tools from the exploit and surveillance tool market, thereby continuing this iterative process.[426]

Security Outputs: iterative security

The assemblage dynamics discussed above have led to a highly unstable security outcome: the devices and applications of Americans are sometimes protected from weak-encryption actors while accessible at other times. The US Encryption Assemblage is therefore characterised by a

[423] James Comey, "The Complexities of Today's Security Challenges" (April 21, 2016), https://aspensecurityforum.org/global/.; Danny Yadron, "'Worth it': FBI Admits it Paid $1.3m to Hack into San Bernardino iPhone," The Guardian, April 21, 2016, http://www.theguardian.com/technology/2016/apr/21/fbi-apple-iphone-hack-san-bernardino-price-paid.
[424] Carman, "An Israeli Company Is Reportedly Helping the FBI Crack the San Bernardino iPhone,"; Selyukh, "The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?"
[425] Samuel Gibbs, "San Bernardino iPhone Hack Won't Work on Newer Models, Says FBI," The Guardian, April 7, 2016, http://www.theguardian.com/technology/2016/apr/07/san-bernardino-iphone-hack-work-newer-models-fbi-james-comey.
[426] Cox, "Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware."

perennial iterative process where advantage alternates between strong and weak-encryption actors, depending on who enjoys what is often a temporary level of technical superiority.

Understanding how these security outputs have arisen involves a variety of factors and variables. Some of which are outside the scope of this thesis – such as the specific technical advantages acceded to both strong and weak-encryption actors. However, the concepts central to an assemblage theoretical framework have a highly influential impact on encryption and security in the US.

Perhaps the most significant variables that have led to such an inconsistent and iterative version of security is the combination of various, and often contradictory, incentive structures alongside a broad distribution of power. This means that power and technical sophistication are distributed between strong and weak-encryption actors. Taking these two variables together is vital – either on its own would lead to stability; the combination of the two, however, breeds disruption. If only one intra-unit cluster had significant technical sophistication, their vision of security would be more likely to dominate, therefore leading to a more stable and consistent version of security prevailing within the assemblage. Likewise, if power was distributed widely but in a structure where the majority of actors had a shared interest in either strong or weak-encryption, then similarly, there would be a more consistent security output.

A second variable that appears significant is the lack of hybridity within the assemblage. As the assemblage dynamics section showed, neither strong, nor weak-encryption clusters are stable, coherent coalitions. Traditional units, including the Government and the private sector are similarly fragmented.

The lack of fusion is exemplified by the fractured nature of both the strong and weak-encryption clusters. Despite sharing a common interest in broad terms, the different actors within each cluster rarely work closely together. While the EFF and Google might both

campaign for strong-encryption, they arrive at the issue from very different places and fundamentally disagree on broader privacy issues for example. Internal divisions are most clearly observed within the US intelligence community. Despite all of the main intelligence agencies (including the NSA, FBI and CIA) being categorized as weak-encryption actors, their differing incentives and institutional models mean that they are not encouraged to work together. With the FBI also a law enforcement actor, its interests in encryption security can also directly contradict those of the NSA.

Although counterfactuals are difficult to establish in social science research, it is at least plausible that were all the actors that sit within either the strong or weak-encryption cluster all collaborating, sharing technical information, and building understanding together, that their vision of security would become stronger and that they would be more likely to achieve a level of sustained dominance within the US Encryption Security Assemblage. This means that fusion is not just an interesting feature of contemporary security structures, but also a variable the clearly impacts security.

Since the release of the Snowden documents, technology firms are aware that it is not only cooperation with US Government actors, but also the perception of cooperation that is important. If technology firms are perceived to be working with US Government actors, they risk damaging their brand and reputation – especially in the context of the global marketplace that they operate in. This creates a dynamic where it is unlikely that the tense relationships and contestation between security actors will be resolved. The iterative security outcome discussed above is therefore likely to sustain in the long-term. This shows that it is vital for security actors to think more deeply about the security structures they are part of and the dynamics that they contain. By understanding an assemblage's characteristics, it then becomes easier to assess negative security outputs and consider how (and if) they might be mitigated in the future. In

this regard, the concepts linked to assemblage thinking contain potentially untapped potential to provide some level of predictive insight.

In some respects, the back-and-forth nature of encryption access reflects the preferences of Americans with ideational backing for strong and weak-encryption often evenly split. Opinion polls provide the best means for measuring individual preferences and the results of different polls provide contradictory information. In the aftermath of Apple's decision to oppose the court order to unlock the iPhone of Farook, a Reuters and ISPOS poll revealed that 46 percent of respondents agreed with Apple's position, 35 percent disagreed and 20 percent said they did not know.[427] Yet, a poll conducted at the same time by the Pew Research Centre revealed that 51 percent of respondents felt Apple should unlock the iPhone to assist the FBI investigation with 38 percent saying they should not and 11 percent unsure.[428] Americans were still divided on the issue in 2017: a further Pew Research Center poll revealed that 46 percent believe that the government should be able to access encrypted communications when investigating crimes, while 44 percent believe that technology companies should be able to use encryption tools that are unbreakable even to law enforcement.[429]

The uncertainty, or at least inconsistency, in the poll data suggests the issue of encryption remains unresolved. It could therefore be argued that given US citizens want different forms of security, the assemblage's iterative security outcome has a degree of democratic

[427] Jim Finkle, "Solid Support for Apple in iPhone Encryption Fight: Poll," Reuters, February 24, 2016, https://www.reuters.com/article/us-apple-encryption-poll/solid-support-for-apple-in-iphone-encryption-fight-poll-idUSKCN0VX159; "Reuters/Ipsos Poll: Apple vs the FBI," Reuters, February 23, 2016, http://fingfx.thomsonreuters.com/gfx/rngs/1/883/1284/APPLE-ENCRYPTION-POLL.jpg.
[428] "More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone" (Washington, DC: Pew Research Center, February 22, 2016), http://assets.pewresearch.org/wp-content/uploads/sites/5/2016/02/2-22-2016-iPhone-release.pdf.
[429] Kenneth Olmstead and Aaron Smith, "Americans and Cyber Security" (Washington, DC: Pew Research Center, January 2017), http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

embeddedness. Broader disagreements around encryption security policy mirror its current iterative security.

The diverging interests of different security actors act as a form of check and balance on each other. Yet, the unstable vision of security has not been developed due to a recognition of the divergences in public opinion or based on some compromise that takes into account individual preferences. The lack of fusion within the US Encryption assemblage means security actors have not engaged with each other or considered broader societal views on the issue. The lack of harmony means that the majority of security actors have not interacted with each other in a spirit of compromise. Very few security providers have taken a full account of the political and security concerns affecting individuals.

Instead, the majority of security providers have pursued a version of encryption security that reflects their own interests, largely due to the highly fragmented nature of the assemblage. This is seen most clearly in the case of profit-motivated technology firms. As previously discussed, while they have taken significant steps to provide strong-encryption, the extent this is due to concern over user privacy is questionable given the way they simultaneously commercialise user data (not that such firms are devoid of ideological principles entirely). A more reasonable assessment would be that these firms are more superficially concerned with data security to the point that it aligns with their own reputation and economic security.

This highlights the influence that fusion can play in developing security outcomes. For instance, it is likely that a greater degree of hybridity between ideologically-motivated and profit-motivated strong encryption actors would lead to profit-motivated actors developing solutions that place a greater emphasis on privacy. Similarly, while the FBI is clearly motivated to protect Americans, the agency operates under an institutional model where it is primarily incentivised to pursue justice in courts – developing means to acquire admissible evidence

therefore triumphs issues of data security or privacy. Yet, it is at least plausible that the FBI would be better able to balance its mandate with broader security issues if it engaged more closely with actors that focus on issues such as data security more directly.

It could be argued that in these circumstances it is civil society actors that must step up – yet even here it is clear that actors including the EFF and ACLU also fall short in considering the full spectrum of security concerns and are perhaps overly dismissive of the intentions and security utility of the intelligence and security community. While Americans might have a considerable number of security providers, there is regularly a deficit between the full spectrum of concerns facing the data security of individuals (such as the appropriate balance between data security and intelligence) and the often-narrower interests of specific security stakeholders.

While these different actors do therefore act as checks on each other to some extent, this does not lead to the democratic embeddedness of broader security principles. Ultimately, security actors in the US Encryption Assemblage pursue their own interests in ways that are potentially detrimental to the interests, security, and privacy of American citizens.

US Encryption Security Assemblage Conclusion

This chapter has shown that a complex and highly diffuse network of actors are involved in US encryption security. The Assemblage Configuration showed that the relevant security actors possess a range of incentive structures, with power dispersed across various actor categories (resided most prominently within technology firms, as well as US intelligence and law enforcement communities). The distribution of power alongside a variety of incentive structures has led to a highly tense and fragmented assemblage dynamic that is likely to sustain in the long-term.

Both of the examples discussed highlighted these tensions, with an emphasis on the rivalry and competition between technology firms and the US intelligence community. This has led to a security output that is in constant flux. The encryption security on US citizens' devices fluctuates as both strong and weak-encryption actors constantly compete.

This case study has also highlighted the unique value of an assemblage approach, when compared to more traditional IR approaches focused on power and interests. From a purely conceptual perspective, an assemblage approach is better able to capture the current dynamics of US encryption debates. While assemblage debates are often framed as a dispute between a pro-encryption private sector and a pro-law enforcement government, an assemblage approach instead prises open 'the government' and the 'private sector'. In doing so, it not only highlights the breadth of viewpoints within each of these traditional units but highlights how new boundaries are emerging based on actors that advocate for either strong or weak encryption. These new networks stray from traditional ontological distinctions and therefore require a theoretical approach that is able to accommodate these empirical realities.

Although understanding the interests and capabilities of different actors forms an important aspect of this case study, an assemblage approach also brings attention to other factors that are critical to security outcomes. This chapter has shown how hybridity and harmony both have an influential bearing on security outcomes. The lack of hybridity within either the strong or weak-encryption cluster is likely one of the main reasons that neither side of the debate has been able to establish dominance. The fragmentation within the assemblage is therefore one of the main reasons why there is an iterative security outcome. Likewise, whilst it is unclear that compromise between strong and weak-encryption actors is even possible, the lack of harmony and the various confrontational practices highlight why neither side has engaged in a collaborative manner. Again, this affects the security outcome of the assemblage. An

assemblage approach highlights the importance of considering relationships between actors in addition to the more traditional areas analysed within IR and security studies such as power and interests.

The clashes between actors act as a natural check and balance on the encryption debate, preventing either side from establishing dominance. In many ways, this mirrors the broader indecisiveness on the issue within the US and could be considered a positive security output. At the same time, however, this iterative security outcome introduces instability and uncertainty while security actors have failed to accommodate the views held by Americans on the issues data security and privacy more broadly.

Encryption disputes represent contentious trade-offs between different versions of security. Two important, yet mutually exclusive, notions of security compete. Straightforward answers do not exist – only imperfect solutions to what are difficult and complex problems.

Chapter Four: The UK Critical National Infrastructure Security Assemblage

Introduction

The vast majority of cyber security actors in the UK CNI Assemblage hope for fundamentally the same outcome – a secure CNI infrastructure. In this regard, there are not the substantial clashing securities where actors have first order disagreements about the definition of security that were observed in the previous case study. This is encouraging as disruption and harm to CNI systems can cause catastrophic impacts which, at their worst, could include the loss of life. Indeed, the security of CNI is a serious concern and the cyber security topic in this thesis that sits closest to traditional 'hard' security issues.

Yet, in addressing the central research question of this thesis, the configuration and dynamics of the UK CNI Assemblage lead to various inefficient and arguably flawed security outputs. Despite various actors sharing a common mission of seeking to secure CNI systems in principle, there is nonetheless divergences in practice for two reasons based on the variables studied in this thesis. First, the study of security actors' incentive structures shows that the security of CNI is typically one of a number of objectives for many security providers. There is an emerging consensus that corporations are underinvesting in cyber security[430] – an issue nowhere more critical than in the case of CNI. While other organisational objectives do not directly clash with securing CNI, they do at least change the extent to which security providers

[430] Reeve, "Industry's Cyber-Security "Market Failure" Must Be Addressed,"; Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," Financial Times

will pursue this aim. It is therefore vital to consider the extent to which security is prioritised within an assemblage. Second, there remains ongoing contestation over what belongs in the public or private sphere within the UK CNI Assemblage as discussed in the Assemblage Dynamics section. Further, as seen with the US case study, with various government actors involved in cyber security (and in the UK case seeking to capture the cyber security issue and remit), the security of UK CNI has caused government departmental rivalry, inefficiency and complexity.

At the core of the UK CNI Assemblage dynamic lies a contradiction. There are significant aspects of both harmony and hybridity in the assemblage as corporations and government actors become increasingly embedded through practices including information sharing, and joint simulation exercises. These close partnerships form a crucial pillar of the UK CNI cyber security response. However, official UK Government strategy has also indicated a need to intervene more directly in the private market.[431] Government actors are therefore both closely partnering and actively challenging the role of corporations simultaneously; how these opposing trends coexist forms a central aspect of this case study.

This case study examines the cyber security of systems associated with CNI in the UK between January 2011 and December 2017. As the following analysis will show, however, the globalising qualities of the cyber domain mean that the case study naturally involves a variety of entities based beyond UK borders. Indeed, the involvement of foreign firms in the UK CNI Assemblage is a central theme explored in one of this chapter's examples.

[431] "National Cyber Security Strategy 2016-2021, HM Government"

A Background of UK Critical National Infrastructure

Much of the CNI in the UK is under the control of supervisory control and data acquisition (SCADA) systems that form the core referent object that the security assemblage of this chapter is based on. SCADA system comprise a multitude of computer-based control systems that allow operators and facility personnel to monitor and control a facility's equipment either locally or remotely.[432] SCADA systems are also used to automate control processes. Small computers known as remote terminal units capture information through sensors (such as pressure gauges or thermometers) and send it back to programmable logic containers that then make adjustments accordingly based on simple logic statements that are programmed in. These mean that, for instance, cooling systems can be automatically engaged when the temperature rises in a power plant, automatically preventing overheating.[433] SCADA systems primarily appeal because of their cost-saving potential as infrastructure firms can reduce both labour and maintenance costs through automation. Likewise, the ability for SCADA systems to identify faults and damages mean that firms can intervene and proactively replace equipment before it escalates to more serious damage.[434] SCADA systems also collect and store a great deal of information for reporting, troubleshooting, and even to demonstrate regulatory compliance.[435] Ultimately, from making sure that the energy supply matches national demand to ensuring that trains run on time, SCADA systems support many aspects of day-to-day life in the UK and in many cases, are critical to the wellbeing of UK citizens and the growth of the UK economy.[436]

[432] "The Advantages of SCADA for Water/Wastewater Treatment Facilities," Shrader Engineering, March 12, 2012, http://www.shrader.net/news/the-advantages-of-scada-for-water-wastewater-treatment-facilities.
[433] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke, "SCADA Security in the Light of Cyber-Warfare," *Computers & Security* 31, no. 4 (June 1, 2012): 418-436. pp. 419-420.
[434] "Internet-Based SCADA: the New Era in Communication Technology," Real Time Solutions, March 17, 2008, http://www.rts.com.np/downloads/whatsscada.pdf.
[435] "The Advantages of SCADA for Water/Wastewater Treatment Facilities."
[436] Nicholson, Webber, Dyer, Patel, and Janicke, "SCADA Security in the Light of Cyber-Warfare," 418.

Despite the benefits of SCADA systems, their potential vulnerabilities make cyber security a pertinent issue to CNI protection. Early versions of SCADA systems have been in place since the 1960s.[437] Yet, the original design, and subsequent evolution of SCADA systems, has failed to account for the possibility of deliberate cyber attacks.[438] Many SCADA systems run on outdated software that is not patched on a frequent basis (if at all) and is thus considerably less secure.[439] In 2009, with Microsoft about to reveal its then latest operating system Windows 7, a number of SCADA systems still used Windows 98 – an operating system designed before viruses had seriously hit the headlines and before many of the electronic threats that exist today were anticipated.[440] There is an additional challenge in integrating physical legacy systems.[441] For critical infrastructure sectors such as energy and water, much of their infrastructure is over 100 years old and was designed at a time when stations that are now remotely controlled were physically manned.[442] This has created another layer of complexity and led to profound security challenges.

In addition to the often-flawed security models of SCADA systems, there are a number of threat actors that could plausibly harm CNI in the UK. At the most dangerous level lies state-associated aggressors that possess deep resources to invest in cyber offensive capabilities. Organised crime and hacker groups also have the potential to undermine CNI. Take the healthcare sector where the criminals have increasingly used ransomware – a type of malware

[437] ibid., 419.
[438] ibid., 418.
[439] A patch is a piece of software designed to update a computer program or its supporting data in order to fix or improve it. This often includes fixing security vulnerabilities and other bugs that could otherwise allow hackers to compromise a system.
[440] Steve Gold, "The SCADA Challenge: Securing Critical Infrastructure," *Network Security* 2009, no. 8 (August 1, 2009): 18–20.
[441] Alvaro A Cardenas et al., "Challenges for Securing Cyber Physical Systems," *Workshop on Future Directions in Cyber-Physical Systems Security*, 2009; Tony Morbin, "Nuclear Weapons Vulnerable to Cyber-Attack Due to Outdated Legacy Systems," SC Magazine, January 22, 2018, https://www.scmagazineuk.com/nuclear-weapons-vulnerable-cyber-attack-due-outdated-legacy-systems/article/1473487.
[442] Interview with William Harvey (Senior Cyber Security Policy Advisor, Cabinet Office) by the author. London, UK. May 28, 2015.

that prevents access to a system, either by locking the system's screen and computers or by encrypting and thereby locking the files and data in a system unless a ransom is paid.[443] The UK is not immune to this trend: in November 2016, a hospital in Northern Lincolnshire cancelled all planned operations and diverted major trauma cases to neighbouring facilities after a virus infected its electronic systems on Sunday. Although the National Health Service (NHS – the publicly funded national healthcare system for the UK), did not reveal the source or nature of the system disruption, cyber security experts have concluded that it is likely to be ransomware from a criminal hacker group.[444] Further, even when threat actors do not have the skill to develop the means to conduct these attacks themselves, there are still opportunities to inflict harm when sophisticated cyber tools produced by other, more sophisticated actors become available. For example, the WannaCry ransomware spread that disabled systems in over forty British National Health Service (NHS) hospitals in May 2017[445] used an exploit known as EternalBlue that was developed by the NSA and then leaked online[446] before being used by North Korea.[447]

A combination of weak security and the presence of threat actors with the resources and motivations to potentially cause harm leads to a number of profound risks for CNI in the UK. At the least malign is brand damage. While a damaged reputation for a UK CNI firm as the result of a cyber attack may be initially thought to be costly for only the firm in question, it is actually much larger given the association between CNI and the UK more generally. If critical

[443] "Ransomware," Trend Micro, accessed January 16, 2017, http://www.trendmicro.com/vinfo/us/security/definition/ransomware.
[444] Brian Krebs, "Computer Virus Cripples UK Hospital System," Krebs on Security, November 2, 2016, https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/.
[445] João Medeiros, "WannaCry Laid Bare the NHS' Outdated IT Network – and it's Still Causing Problems," Wired, May 24, 2017, http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware.
[446] Matt Burgess, "Everything You Need to Know About EternalBlue – the NSA Exploit Linked to Petya," Wired, June 28, 2017, http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.
[447] Lord Ahmad, "Foreign Office Minister condemns North Korean actor for WannaCry attacks," GOV UK, December 19, 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

infrastructure in the UK is regarded as insecure, this may deter future foreign investment. There can also be significant financial implications for both the CNI organisation in question and the economy more broadly. A fault in a SCADA system in a power grid in the North East of the US led to a power outage that cost between $4 and $10 billion. Although the power outage was not caused by a malicious actor, the incident nonetheless showed the impact of compromised SCADA systems.[448] Whether a public of private organisation, financial damage to a CNI organisation is likely to hurt consumers – either through increased costs or a reduced service.[449] Further and most serious of all is a loss of life indirectly – through attacks on hospital systems or the energy grid for example.[450]

Given these realities regarding the security of CNI, it is no surprise that there have already been various politically disruptive incidents where cyber attacks have been used to target CNI. A US-Israeli cyber operation known as Stuxnet is the best example of the destructive potential of a cyber attack. The Stuxnet malware manipulated valves on the centrifuges of an Iranian nuclear plant, increasing the pressure inside the centrifuges and damaging the devices as well as the enrichment process.[451] It is estimated that the malware destroyed up to 1000 centrifuges. The incident set back the progress of Iran's nuclear development and no doubt provided an important message to the Iranian government about the US and Israel's capabilities.[452] A less widely publicised, yet still disturbing, attack was conducted on the SCADA systems of a

[448] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," (U.S.-Canada Power System Outage Task Force, April 2004).
[449] In the case of public services, costs may be in addition recuperated through higher taxes or cuts to other public services, thereby leading to a clear opportunity cost as a result of a cyber attack.
[450] For example, the North East power outage mentioned above resulted in eleven deaths. See, Nicholson, Webber, Dyer, Patel, and Janicke, "SCADA Security in the Light of Cyber-Warfare," 423.
[451] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Broadway Books, 2015); Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," February 2011.
[452] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" (Washington, DC: Institute for Science and International Security, December 22, 2010).

German steel mill in 2014, causing a blast furnace to shut down and resulting in significant damage.[453] There have also been other attacks on the Ukrainian power grid and attempts to penetrate the system of a dam in New York[454] that have led to cause for concern. More recently a cyber attack targeting a Saudi Arabian petrochemical company plant was designed not to destroy data or shut down the plant but to trigger a lethal explosion.[455] Whilst some of these incidents have provoked various sensationalist claims warning of a 'cyber Pearl Harbour' or 'cyber 9/11' that have been rightly critiqued by academia as unhelpful,[456] they nonetheless illustrate the material damage that cyber attacks can, and will continue, to inflict.

The cyber security outlook of UK CNI requires ongoing evaluation given a dynamic and quickly changing landscape. UK government actors have prioritised various initiatives including building an 'internet of things' ecosystem,[457] and the development of 'smart cities' and 'smart grids' that are increasingly connected online (and thereby potentially vulnerable to attack).[458] The importance of cyber attacks is now acknowledged in official UK security policy: the UK National Security Strategy and Strategic Defence and Security Review classified cyber attacks as a Tier One threat to national security – above those such as organised crime and attacks using chemical, biological, radiological or nuclear weapons.[459] The strategy document warned that a 'growing numbers of states, with state-level resources, are developing advanced

[453] Kristan Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," *International Affairs* 92, no. 5 (August 29, 2016): 1079-1105. pp. 1090.
[454] Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," The New York Times, March 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.
[455] Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," The New York Times, March 16, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.
[456] Thomas Rid, *Cyber War Will Not Take Place*, (London, UK: Hurst, 2013); Brandon Valeriano and Ryan C Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, (New York: Oxford University Press, 2015).
[457] The Internet of Things refers to the increasing number of everyday objects, from thermometers to fitness watches, that are now connected online.
[458] Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," pp. 1103.
[459] "National Security Strategy and Strategic Defence and Security Review 2015," (London, UK: HM Government, November 22, 2015). pp. 87.

capabilities which are potentially deployable in conflicts, including against CNI and government institutions.[460]

Assemblage Configuration: corporation-led security and public-private fusion

This following section outlines the security actors involved in the UK CNI cyber security assemblage, as well as their incentive structures and capabilities. Four of the traditional units outlined in Chapter Two are discussed: corporations, government actors, international actors, and academic actors.

While there are a significant number of actors involved in the UK CNI Assemblage (given its scale), there are broadly straightforward instances of clustering. In many ways, the traditional units of corporations and the UK Government provide helpful, yet it is the fusion between the two that forms the prevailing inter-unit cluster. It is these instances of public-private partnership that form a significant amount of the analysis in the following sections. However, given that almost all corporations and government actors are involved in such partnership arrangements, the following outline avoids assigning actors into any inter-unit clusters (in the way Chapter Three assigned groups into the strong or weak encryption interunit cluster for example).

Government Actors

The UK government picture is noticeably decentralised with range of government actors providing cyber security to UK CNI in some form. A 2015 UK security strategy review acknowledges this reality, stating that 'responsibilities for infrastructure policing are shared

[460] ibid., pp. 19.

across several organisations with different levels of capability and capacity, and different arrangements for funding, oversight, regulation and legislation.'[461]

The Cabinet Office leads the overall cyber security strategy of the UK that includes the protection of UK CNI. Historically, the responsibility for cyber security was vested in the Home Office but the role moved to the Cabinet Office in 2009 to facilitate a response that focused on cyber security in a broader sense, including a focus in in areas traditionally outside the purview of the Home Office including education and training.[462] Within the Cabinet Office, the Office of Cyber Security & Information Assurance (OCSIA) is the primary office tasked with cyber security and assists Cabinet Office ministers and those and at the National Security Council in determining priorities.[463] The unit writes the UK Cyber Security Strategy and provides strategic direction and coordination over the cyber security programme for the UK government.[464] From a crisis management perspective, including in the event of a serious cyber attack on UK CNI, the UK Cabinet Office Briefing Room (COBRA), acts as the central crisis management response mechanism for crisis situations. Similar to the United Kingdom's conventional response to crisis situations, however, responsibility for a cyber crisis situation rests with the relevant government departments.[465] Given that the Cabinet Office provides the strategic lead for cyber security, the Prime Minister's Office generally plays a largely hands-off role according to one interviewee who worked at the OCSIA.[466] While the Prime Minister will sign off on government strategy, they will not necessarily be directly involved in the

[461] "National Security Strategy and Strategic Defence and Security Review 2015," (London, UK: HM Government, 2015). pp. 44.
[462] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom"; Anna-Maria Osula, "National Cyber Security Organisation: United Kingdom," (Tallinn, Estonia: NATO CCDCOE, 2015).
[463] "Office of Cyber Security and Information Assurance," GOV UK, accessed March 16, 2017, https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.
[464] ibid.
[465] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."
[466] Interview with William Harvey.

process. In the event of a serious cyber attack on CNI, the Prime Minister will chair COBRA and coordinate a response – this would include working with the relevant government actors or departments, as well as other duties such as speaking to the media.

Each of the thirteen UK national infrastructure sectors has one or more lead government department that is responsible for the sector and ensuring that the cyber security of the sector is appropriately secured.[467] This means, for example, that the Department of Health is responsible for cyber attacks that target hospitals while the Department for Energy and Climate would be responsible for the security of energy infrastructure such as the power grid. The CPNI states that 'Government departments have lead responsibility for ensuring appropriate steps are taken within their sectors to improve protective security. They also lead on the identification of critical infrastructure within their sectors in consultation with CPNI and sector organisations.'[468] This means that all government departments that contain a CNI component have some level of responsibility for cyber security of CNI systems.

Devolution further complicates the configuration of government security actors: Scotland has power for health, policing, the fire service and aspects of transport; Northern Ireland for health and policing; and Wales for health, fire and rescue, and highways and transport.[469] The list of security providers is complicated further by the fact that water boards, health-care trusts and local councils have their own sets of responsibilities and reporting in some areas.

UK intelligence agencies play an important role in protecting the cyber security of UK CNI.[470] GCHQ, the UK government signals intelligence agency is seen by government as the most

[467] Carr, "Public–Private Partnerships in National Cyber-Security Strategies," pp. 53.
[468] "Critical National Infrastructure"; Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," pp. 1089.
[469] ibid., 1097.
[470] ibid., 1099.

substantial source of expertise. This was acknowledged by the then Chancellor George Osbourne in November 2015 where, in a speech at GCHQ's headquarters, Osbourne stated:

> *'I am clear that the answer to the question "who does cyber?" for the British government is – to a very large degree – "GCHQ"....GCHQ has a unique role. It is the point of deep expertise for the UK government. It has an unmatched understanding of the internet and of how to keep information safe. It is a centre of capability that we cannot duplicate, which must sit at the heart of our cyber security."*[471]

From a UK CNI perspective, GCHQ provides guidance and tailored advice to the UK government regarding CNI and the security risks of both new and existing IT systems – as well as developing strategies to protect against these risks.[472] Both MI5 and MI6, the UK's respective domestic and foreign human intelligence agencies, also claim cyber security as part of their remit. However, given the more clandestine nature of these intelligence agencies (when compared to GCHQ), their precise role in the protection of UK CNI is less well understood.

Perhaps the clearest contribution to cyber security and the protection of UK CNI comes from the National Cyber Security Centre (NCSC) that was launched in 2016. The NCSC sits within GCHQ[473] and its remit is to acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security. GCHQ has previously been the main intelligence agency to lead the cyber security effort, given the relevant skills and experience of those who have worked in signals intelligence. Yet while agencies such as GCHQ possess the capability to tackle cyber security, they are also a covert organisation. This is in

[471] George Osbourne, "Chancellor's Speech to GCHQ on Cyber Security," GOV UK, November 17, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.
[472] Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," pp. 1093.
[473] The previous arm of GCHQ responsible for cyber security, the Communications-Electronics Security Group is now part of the NCSC.See "CESG," GOV UK, accessed February 2, 2016, https://www.gov.uk/government/organisations/cesg.

stark contrast to the culture required to confront the cyber security challenge, which requires instead a more open and communicate response towards both other government actors as well as corporations and international actors.[474] The NCSC corrects this position by bringing those with the necessary skill set to tackle the cyber security challenge out of the shadows.[475] The centre will therefore tap directly into the skills and resources of GCHQ, but will translate this into a more publicly facing organisation. From a UK CNI point of view, the NCSC will have partial responsibility along with the relevant government departments outlined above for the protection of UK CNI IT networks, data and systems from cyber attacks.'[476]

The NCSC also brings together and incorporates various government bodies that were previously distinct. For example, both CESG (the part of GCHQ that previously looked at cyber security) and the Centre for Cyber Assessment are now part of NCSC. The UK-national computer emergency response team (CERT-UK) is also now part of the NCSC.[477]

The Centre for the Protection of National Infrastructure (CPNI) has a remit to provide guidance and expert advice to UK CNI actors. From a cyber security perspective specifically, the main focus of the CPNI is to prevent cyber attacks on CNI by recommending security controls and offering advice on how to avoid crisis situations occurring. While necessary, the preventative emphasis of the CPNI means that the organisation has a limited role when serious attacks on UK CNI occur.[478] Within this role, however, the CPNI has achieved a strong network of security-cleared contacts that can be utilised in the event of a crisis.[479] As the then Defence

[474] Collier, "Getting Intelligence Agencies to Adapt to Life Out of the Shadows."
[475] ibid.
[476] "Critical National Infrastructure."
[477] "New National Cyber Security Centre Becomes Operational," GCHQ, October 4, 2016, https://www.gchq.gov.uk/news-article/new-national-cyber-security-centre-becomes-operational.
[478] Wayne Harrop and Ashley Matteson, "Cyber Resilience: a Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA," *Journal of Business Continuity Emergency Planning* 7, no. 1 (March 7, 2014): 149–62.
[479] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."; Harrop and Matteson, "Cyber Resilience: a Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA.".

Secretary, Phillip Hammond told the Defence Select Committee in October 2013, CPNI is 'where the impacts of cyber issues and cyber attacks on the broader national infrastructure are worked through, so that the vulnerabilities of utilities and other services that might be impacted by an attack on critical networks can be worked through and defensive strategies put in place.'[480]

It should be emphasised that the outline above is an overview of the key government actors that are involved specifically with UK CNI. Other government departments (including the National Crime Agency and the Foreign and Commonwealth Office) include cyber security in their remit. In fact, given the prevalence of the cyber domain, cyber security is increasingly becoming part of all sorts of government actors' purview. Although these agencies are not tasked with protecting UK CNI directly, the issue may of course come up tangentially. Having provided an overview of the key government actors, the complexity of an often highly decentralised system becomes apparent.

Despite an impressive cyber security capability when compared to other governments, the UK Government has been unable to compete with the salaries on offer in the private sector. Even GCHQ, a government actor that possesses a significant share of government talent has struggled with its employees being reported to be able to triple their salary by leaving to established tech firms such as Microsoft, Google, and Apple[481] that has challenged the agency's strategic thinking.[482] Former GCHQ Director Iain Lobban even suggested that the intelligence

[480] "Towards the next Defence and Security Review: Part One, 7th Report of Session 2013–14," (London, UK: House of Commons Defence Committee, December 18, 2013), https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/197/197.pdf; Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," pp. 1097.
[481] Kelly Fiveash, "GCHQ Losing Its 'Internet Whizzes' to Microsoft, Google," The Register, July 14, 2011, https://www.theregister.co.uk/2011/07/14/gchq_microsoft_google/.
[482] Former GCHQ Director Iain Lobban suggested that the agency might have to reconsider its requirement that it only hires British nationals. It has also been proposed that the agency creates programs that seek to attract employees for a short-term period (around two years) before going on to other careers. See Duncan Gardham, 'Whizz Kids Deserting the Spy World as Threat of Attacks Increases,' The Telegraph, July 13, 2011, http://www.telegraph.co.uk/news/uknews/terrorism-in-the- uk/8635959/Whizz-kids-deserting-the-spy-world-as-

agency might have to consider hiring foreign-based talent.[483] Although this has never materialised, that it was even floated as an option by a clandestine intelligence agency speaks volumes to the recruitment challenges at hand. Further, although GCHQ – the central locus of UK government cyber security talent – is involved in the protection of CNI, it is not the agency's central mission. GCHQ's traditional mission has been intelligence gathering[484] – an activity that requires materially different resources to those required to protect CNI. Further, government actors that that do not specialise in cyber security experience face an even more severe skill shortage. With so many government actors in need of cyber security skills, from the department of health to the Cabinet Office, any influx of talent is soon diluted. Further, for many government departments, acquiring the necessary skills and resources is simply not prioritised. For example, the 2017 WannaCry ransomware spread affected systems in over forty British National Health Service (NHS) hospitals as a result of outdated software.[485] Many NHS computers were still running Windows XP – an operating system initially released in 2001 that has been replaced many times over. Although running up-to-date software features is routine security advice, in a resource-constrained environment, other issues may be prioritised instead. For managers and government officials faced with many budgetary concerns, a delay to a time-consuming, costly, and uncertain update programme may seem a rational decision.[486]

Yet, UK Government actors' capabilities should not be dismissed entirely. Although it is true that the traditional primary mission for GCHQ has been intelligence gathering, this is still of direct relevance to cyber security: those adept at breaking into systems (for intelligence

threat-of-attacks-increases.html; Oliver Wright, "GCHQ's 'Spook First' Programme to Train Britain's Most Talented Tech Entrepreneurs," The Independent, January 1, 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/gchqs-spook- first-programme-to-train-britains-most-talented-tech-entrepreneurs-9953516.html.

[483] Gardham, "Whizz Kids Deserting the Spy World as Threat of Attacks Increases," The Telegraph.

[484] Aldrich, *GCHQ*.

[485] João Medeiros, "WannaCry Laid Bare the NHS 'Outdated IT Network – and It's Still Causing Problems," *Wired*, May 24, 2017, http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware.

[486] Collier and Martin, "Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand."

gathering) learn, by extension, what makes a system secure or not. Whilst government actors cannot compete on pay with corporations, government actors have responded with competitive non-salary benefits that feature prominently in their recruitment message. Flexible working hours and generous holiday allowances are mentioned as a part of these agencies' family-friendly work environment while a significant investment in employee education and training reassures potential recruits that they can further develop their skills and career capital by joining.[487] The UK executive has also recognised the importance of cyber security as an issue: starting with a five-year budget of £650 million in 2011[488] (and an additional investment of £210 million in 2013),[489] cyber security spending has since doubled with £1.9 billion pledged for the period of 2016-2021.[490] This increased spending has been reflected in recent initiatives including the creation of the NCSC.

Corporations

Around 80 percent UK CNI is owned and managed by private sector firms[491] and they therefore form a significant proportion of the total number of CNI security actors. A range of different sort of corporations are involved, all with their own set of characteristics and incentive structures, including: UK-based private sector firms, multinational companies (both UK and foreign based), quasi-private firms, and state-owned firms.

Even amongst UK private firms specifically, there is significant variety in the type of firms that operate. This is reflected through a range of ownership structures. An examination of water suppliers provides a case in point. Youlgrave Water is an example of a private limited firm that

[487] ibid.
[488] "Government Publishes Cyber Security Strategy," GOV UK, September 25, 2011, https://www.gov.uk/government/news/government-publishes-cyber-security-strategy.
[489] Francis Maude, "UK Cyber Security Strategy: Statement on Progress 2 Years on," December 12, 2013, https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-2-years-on.
[490] "Britain's Cyber Security Bolstered by World-Class Strategy."
[491] Ashford, "Is UK Critical National Infrastructure Properly Protected?"

is independently owned and managed by members of the local Youlgrave community. These sort of firms do not follow traditional business incentives: Youlgrave Water is a non-profit, its directors do not receive fees or salaries and it is run solely for the benefit of local residents.[492] Firms such as Portsmouth Water and South Staffordshire Water are also private limited companies but run on a for-profit basis.[493] Other firms such as Dee Valley Water and Severn Trent Water are publicly listed companies – Severn Trent Water is even large enough to be on the FTSE 100. For many of these publicly listed companies, the majority of their shares are owned by large multinationals or banks. For example, Affinity Water is owned by a consortium led by Infracapital Partners (an infrastructure fund owned by M&G Investments) and North Haven Infrastructure Partners (an infrastructure fund owned by Morgan Stanley).[494] Both profit driven privately limited firms and publicly listed companies follow a similar set of incentives, although it should be realised that the makeup of the shareholders may change an organisation's behaviour (for example, in determining whether short or long-term business strategies are favoured).

The divergence in the scale of these firms is also reflected not just through their ownership and incentive structures but also through the coverage that they provide. Staying with the example of water supply, there is a range of local, regional and national providers. For example, Portsmouth Water's coverage extends to only Portsmouth and a few surrounding towns on the South Coast.[495] By contrast, United Utilities and Yorkshire Water provide water to the entire North-West and Yorkshire regions respectively.[496] Coverage also extends to entire countries

[492] "Youlgrave Waterworks Ltd: a Brief History," Youlgrave Waterworks, accessed October 3, 2017, http://www.youlgrave.org.uk/?page_id=51.
[493] "Company Overview of Portsmouth Water Limited," Bloomberg, October 11, 2017, http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=12505401.
[494] "Agreed Sale of Affinity Water," (Morgan Stanley and Infracapital, May 2, 2017) https://www.infracapital.co.uk/Controls/Brochure/-/media/Infracapital/PDFs/Press%20Releases/Infracapital-agrees-sale-of-Affinity-Water.pdf.
[495] "Our Company," Portsmouth Water, accessed October 5, 2017, https://www.portsmouthwater.co.uk/about-us/.
[496] "About Us," United Utilities, accessed October 5, 2017, https://www.unitedutilities.com/help-and-

with Scottish Water providing water to the whole of Scotland.[497] Out of all the firms involved in water supply, all bear some responsibility for the provision of cyber security. Given the differences in resources and scale, the cyber security capability and the challenges different firms face is likely to be highly divergent.

As well as CNI organisations themselves, a range of private sector contractors and other organisations are involved in their day-to-day running. This includes, for example, caterers, physical security services, etc.[498] CNI organisations will often source their hardware and software from external private sector firms, thereby increasing the complexity of the supply chain relevant to cyber security. In addition to these suppliers, there are also a number of cyber security contractors and consultancies that are used. These cyber security organisations work with clients within various industries including CNI organisations and help them to establish effective cyber security strategies and protocols. Although some of these cyber security organisations are UK private sector firms,[499] others are larger multinational partnerships[500] and companies[501] – a category of private firm examined below. These diverse supply chains and use of third parties drastically increases the complexity and scale of the UK CNI Assemblage.

While some of the UK private firms outlined above are owned by multinational companies, portions of UK CNI are also managed directly by multinational corporations. National Grid is a British multinational corporation that runs the electric power transmission in the UK that connects power stations to households and businesses.[502] While National Grid is headquartered in Warwick, UK the firm also runs a significant portion of the power transmission network in

support/about-us/; "About Us," Yorkshire Water, accessed October 5, 2017, https://www.yorkshirewater.com/about-us.

[497] "About Us," Scottish Water, accessed October 5, 2017, http://www.scottishwater.co.uk/about-us.

[498] "Mitigating Security Risk in the National Infrastructure Supply Chain," (London, UK: CPNI, June 2017).

[499] For example, Templar Executives and C3IA.

[500] For example, PwC.

[501] For example, BAE Systems.

[502] Interview with National Grid employee by the author. Warwick, UK. May 13, 2015; "About National Grid," National Grid, accessed October 5, 2017, http://www2.nationalgrid.com/About-us/.

the Northeast of the United States.[503] The firm has a primary listing on the London Stock Exchange and is a constituent of the FTSE 100 index but also has a secondary listing on the New York Stock Exchange.[504] A portion of the National Grid cyber security team is centralised, with the same personnel tasked with securing the networks of both the UK and US national grid according to an interviewee that worked at the organisation in the cyber security team.[505] The Chief Information Security Officer is a position that is responsible for both the UK and the US for instance. There are other examples of UK based multinationals providing key portions of UK CNI and thus also responsible for the cyber security of UK CNI. For example, British Telecom is a telecommunications service provider that operates in over 180 countries. This does not necessarily alter the incentives for protecting the UK, but does bring up questions about how such organisations work in a global context and how the various subsidiaries in their business work together.

The role of multinational corporations in the provision of CNI and cyber security specifically has led to controversy. Huawei is one of the largest providers of telecommunication equipment in the UK and has deals in place to provide CNI as well as the technology behind services for a number of companies' UK operations including BT, EE, Virgin Media, O2 and Sky. The company, which was founded by a former military technologist from the Chinese army,[506] provides services across all aspects of the telecom's infrastructure chain, including the technical boxes and masts that carry voice and data communications to the software that runs the network and the handsets that receive calls.[507]

[503] ibid.
[504] "Shareholder Centre," National Grid, accessed October 5, 2017, http://investors.nationalgrid.com/shareholder-centre.aspx.
[505] Interview with National Grid employee.
[506] Sam Jones and George Parker, "GCHQ Seeks to Allay Hinkley Security Fears," Financial Times, October 16, 2015, https://www.ft.com/content/d3fc0cb6-740c-11e5-a129-3fcc4f641d98.
[507] James Blitz and Daniel Thomas, "Parliamentary Report Raises Alarm Over Lack of Checks on Huawei," Financial Times, June 6, 2013, https://www.ft.com/content/d3680d06-cecb-11e2-8e16-00144feab7de.

Aspects of UK CNI are also owned and managed by firms with strong links to government actors. The provision of electricity provides a case in point. When electricity generation was privatised, the UK public sector company London Electricity was sold in 1996 to Entergy 1996, a US firm. Two years later, it was sold to Électricité de France (EDF) before EDF Energy was established as the UK arm of EDF but is owned and controlled by its French parent company – a company largely owned by the French state.[508] Portions of UK CNI are also managed or even owned by purely state-owned corporations. The Chinese state corporation named China General Nuclear Power Corporation will invest around £6 billion – a third of the money for a new nuclear plant at Hinkley Point in Somerset that will meet seven percent of the UK's electricity needs (with EDF paying for the other two thirds).[509] China General Nuclear Power Corporation has agreed to take on such an investment on the understanding that the UK government would also approve a Chinese-led and designed nuclear power plant at Bradwell in Essex.[510]

Corporations are predominantly financially motivated. They seek high profits by increasing or maintaining revenue while ensuring that costs are kept low.[511] Corporations may also have other motivations: a private sector firm may seek to grow or expand into new markets and this might involve an increase in costs in the short or medium term. Corporations may also have political motivations. Yet, for the purpose of CNI cyber security actors, it is broadly reasonable to assume that corporations seek to maximise profit. In many respects, the state-owned

[508] Alex Brummer, *Britain for Sale: British Companies in Foreign Hands – the Hidden Threat to Our Economy*, (New York: Random House, 2012) pp. 143-144.
[509] "Hinkley Point: UK Approves Nuclear Plant Deal," BBC News, September 15, 2016, http://www.bbc.com/news/business-37369786.
[510] George Parker and Christopher Adams, "UK Paves Path for West's First China-Designed Nuclear Reactor," Financial Times, September 21, 2015, https://www.ft.com/content/52462048-5f8b-11e5-a28b-50226830d644?mhq5j=e5.
[511] Myriam Dunn-Cavelty and Manuel Suter, "Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection" 2, no. 4 (December 1, 2009): 179–87; Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016): 43–62.

corporations discussed above (including EDF and China General Nuclear Power Corporation) share these traditional business motivations. Yet, they may also face an additional set of incentives based on the strategy of their home government. With the Chinese government having established ambitious plans to expand its influence around the world, its state-owned firms form a pillar of this strategy.[512]

Corporations that own and manage CNI have various interests in ensuring the cyber security of CNI. Cyber security is clearly an increasingly important component within business strategy with cyber attacks and data breaches exposing a business to several challenges. They can easily damage a corporation's reputation and undermine consumer confidence. High-profile cyber incidents have previously cost executives their jobs when they have been forced to resign in the aftermath of a serious incident.[513] Likewise, when an organisation has been negligent in regards to cyber security, there can be negative legal implications with customers suing the organisation in question.[514]

Yet, it should also be realised that delivering robust and secure systems can at times conflict with other business objectives. For organisations seeking to keep costs low, cyber security investments risk becoming side-lined. Although share prices often fall in response to a data breach, this is often only temporary, leading to questions as to the extent to which executives are incentivised to prevent cyber attacks.[515] This leads to a tension: owners of CNI want to ensure that they have a good level of cyber security, yet also have competing business

[512] Ilan Alon et al., "Chinese State-Owned Enterprises Go Global," *Journal of Business Strategy* 35, no. 6 (2014): 3–18.
[513] Eric Basu, "Target CEO Fired - Can You Be Fired if Your Company Is Hacked?," Forbes, June 15, 2014, https://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/#1dea5f7e7c9f.
[514] Ben McLannahan, David J Lynch, and Chloe Cornish, "Equifax Shares Drop as Questions Mount Over Data Breach," Financial Times, September 8, 2017, https://www.ft.com/content/f503ef3c-94b2-11e7-a9e6-11d2f0ebb7f0?mhq5j=e5.
[515] Elena Kvochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, March 31, 2015, https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

objectives. While these business objectives do not directly encourage bad cyber security, they are likely to reduce the incentives of implementing cyber security.

Corporations are, however, able to hire those with relevant cyber security skills – a challenge given the current cyber security skill shortage in the UK. The dearth of those with the relevant cyber security skills and expertise has pushed wages up – private corporations have been the security actors with the economic resources to recruit this talent. Of course, not all of those with in-demand skills work in CNI organisations. Many will work for cyber security contractors and consultancy firms. Others will simply work in the technology sector but not in the cyber security industry – working for Apple to develop the next generation of iPhones for example. However, out of the limited supply of skilled talent, CNI organisations are competitive in their ability to recruit talent.[516] When these organisations require additional support, they have the economic resources to bring in cyber security contractors and consultancies to supplement their permanent staff, thereby increasing their overall access to relevant human capital.[517] Corporations also have the resources to purchase the necessary computer capital. Technology firms invest substantially on research and development. Cyber security firms that work alongside the owners and managers of CNI dedicate resources to keeping up-to-date databases of threat intelligence, used in threat detection and network monitoring software.

Corporations have long enjoyed public and political support for their role as CNI providers. As an economy that puts faith in market mechanisms, there is an established culture of industries being privatised that adds to the ideational weight behind private sector management. This process was exemplified by Thatcher, with it being argued that her most significant legacy

[516] Interview with William Harvey.
[517] ibid.; interview with cyber security consultant (a) (working with UK Government clients) with the author. London, UK. May 21, 2015.

being the privatisation of state-owned industries.[518] Setting out a bold vision of 'rolling back the frontiers of the state,'[519] £60 billion of state assets were sold with a number of CNI actors privatised including British Gas and various water companies.[520] The extent of the ideational weight behind private sector management is reflected in the following decades with Thatcher's successor, Prime Minister John Major also selling off government owned CNI assets including electricity transmission and distribution companies in 1991 as well as Railtrack in 1997.[521] Having initially opposed the Conservative government's privatisation programme, the Labour party moved first to acceptance and then to endorsement.[522] Indeed, commenting on Thatcher, Labour Prime Minister Tony Blair claimed that 'I always thought my job was to build on some of the things she had done rather than reverse them.'[523] Since then, various Conservative and Conservative-coalition governments have maintained current levels of privatisation.[524]

Yet, the ideational support for privatised CNI is also being questioned more recently. Current Labour party leader Jeremy Corbyn performed better than expected in the 2017 UK General Election, with his campaign manifesto proposing the renationalisation of key public services including rail and energy firms.[525] A 2017 YouGov pol confirms that public sentiment in the UK is shifting with sixty percent of those surveyed supporting rationalisation of rail companies

[518] Mike Toms, "The Thatcher Privatisation Legacy: Not Quite What She Planned?" (London, UK: Oxera Agenda, May 2013).
[519] Nigel Lawson, "Economy: The New Conservatism" (August 4, 1980), https://www.margaretthatcher.org/document/109505.
[520] Toms, "The Thatcher Privatisation Legacy: Not Quite What She Planned?"
[521] ibid.
[522] Aimee Oakley, "New Labour and the Continuation of Thatcherite Policy," *POLIS Journal* 6 (2011): 1–37.
[523] "Tony Blair: 'My Job Was to Build on Some Thatcher Policies'," *BBC News*, April 8, 2013, http://www.bbc.co.uk/news/av/uk-politics-22073434/tony-blair-my-job-was-to-build-on-some-thatcher-policies.
[524] Emma Simon, "Thatcher's Legacy: How Has Privatisation Fared?," The Telegraph, April 12, 2013, http://www.telegraph.co.uk/finance/personalfinance/investing/shares-and-stock-tips/9989430/Thatchers-legacy-how-has-privatisation-fared.html; Chris Edwards, "Margaret Thatcher's Privatization Legacy," *CATO Journal* 37, no. 1 (February 1, 2017): 89–101; Patrick Wintour, "Margaret Thatcher's Political Legacy Remains Impossible to Avoid," The Guardian, April 8, 2013, https://www.theguardian.com/politics/2013/apr/08/margaret-thatchers-political-legacy.
[525] Anushka Asthana and Heather Stewart, "Labour Party's Plan to Nationalise Mail, Rail and Energy Firms," The Guardian, May 11, 2017, https://www.theguardian.com/politics/2017/may/10/labour-party-manifesto-pledges-to-end-tuition-fees-and-nationalise-railways.

and fifty nine and fifty three percent respectively for watt companies and energy companies respectively.[526] Private sector involvement in CNI and cyber security has been most controversial on issues related to outsourcing and foreign-based firm involvement. There has been concern raised surrounding Huawei's role in CNI with MI5 (the UK domestic intelligence agency) stating the theoretical potential for the Chinese state to exploit vulnerabilities in Huawei equipment to intercept or disrupt UK communications.[527] Government outsourcing to corporations has also been controversial. The level of outsourcing within the Single Intelligence Account was criticised by the Intelligence and Security Committee that launched an investigation on the basis that this was leading to excessive costs.[528]

International Actors and Networks

The assemblage framework used in this thesis argues that binary global-local distinctions are less useful for framing national security. In the context of UK CNI, this has already been demonstrated by the presence of global firms outlined in the previous corporation section becoming deeply embedded in aspects of what is central to matters of UK national security. The overlapping of global and local security actors becomes further apparent when international actors and networks, such as state partners and International Governmental Organisations (INGOs), are considered.

CERTs from across the world cooperate through the Forum of Incident Response and Security Teams (FIRST). This network provides a forum for information exchange and cooperation on

[526] Matthew Smith, "Nationalisation vs Privatisation: the Public View," YouGov, May 19, 2017, https://yougov.co.uk/news/2017/05/19/nationalisation-vs-privatisation-public-view/.
[527] Sir Malcolm Rifkind, "Intelligence and Security Committee: Annual Report 2011-2012," (London, UK: Intelligence and Security Committee, July 5, 2012).
[528] ibid.

issues of mutual interest.[529] The network brings together CERTs from government, business and academia. Within its mission statement, the FIRST network seeks to help members develop and share technical information, tools, methodologies, processes and best practices.[530] It all promotes the creation and expansion of incident response teams.[531] Within the UK, a range of CERTs are involved in the FIRST network including the NCSC as well as various private CNI corporations including the National Grid and British Telecom amongst others.[532]

CERT cooperation also occurs at the European level. After a successful one-year pilot, the EU has set up a permanent CERT (CERT-EU) for EU institutions, agencies and bodies.[533] CERT-EU cooperates closely with other member state CERTS including CERT-UK.

The UK FCO has a cyber policy unit that sends a representative to the United Nations (UN) Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[534] The UN GGE is a UN-mandated working group in the field of information security.[535] Through multilateral meetings, state representative at the UN GGE have tried to cultivate and agree on cyber norms.[536] The thinking behind this has been to establish rules of the road in the cyber domain. This has included agreements that principles such as international law, state sovereignty and the

[529] "iOS Security," (Cupertino, CA: Apple, March 16, 2017).
[530] "FIRST Vision and Mission Statement," FIRST, accessed October 10, 2017, https://www.first.org/about/mission.
[531] ibid.
[532] "FIRST Teams," FIRST, accessed October 10, 2017, https://www.first.org/members/teams/.
[533] "About Us," CERT EU, accessed October 10, 2017, https://cert.europa.eu/cert/plainedition/en/cert_about.html.
[534] "UN GGE," Geneva Internet Platform Digital Watch, accessed October 10, 2017, https://dig.watch/processes/ungge.
[535] ibid.
[536] ibid; Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms Legal, Policy Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn, Estonia: NATO CCDCOE, 2016), 87–109.

settlement of disputes by peaceful means are principles that are transferable in the cyber domain.[537]

The cyber norms established at the UN GGE are directly relevant to UK CNI. Here, the issue of the CNI norms has developed substantially. The 2010 UN GGE report recommendations for 'further dialogue among states to reduce the risk and protect critical national and international infrastructure'.[538] While this initial agreement initially sought to reach consensus on the need for states to improve their cyber defences, the 2015 report went much further by seeking to limit the offensive activity of other states. One of the limiting norms of the 2015 UN GGE Report states that governments 'should not conduct or knowingly support ICT activity that potentially damages critical infrastructure.[539] The report also established that states should not harm other states' authorised CERTS.[540] Such norms are clearly an alternative form of security provision: rather than seeking to provide or improve cyber defences, initiatives at the UN GGE instead attempt to reduce the likelihood and severity of the threat at hand. However, in June 2017, UN GGE members failed to reach a consensus for the first time since 2004-05.[541] While this certainly shows that such norm building exercises have a limited scope for producing change, the current lack of serious and persistent state-on-state cyber attacks on CNI would mean that it is at least arguable that the previous agreements and discussions have helped to build an understanding amongst governments regarding the targeting of CNI.

[537] "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations Office for Disarmament Affairs, accessed October 10, 2017, https://www.un.org/disarmament/topics/informationsecurity/.
[538] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Sixty-Fifth Session," pp. 2.
[539] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," (United Nations, August 18, 2015).
[540] ibid.; Elaine Korzak, "The 2015 GGE Report: What Next for Norms in Cyberspace?," Lawfare, September 23, 2015, https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.
[541] Grigsby, "The End of Cyber Norms."

As a member of the North Atlantic Treaty Organisation (NATO), the UK is also linked to the security provision of NATO. In July 2016, NATO member states affirmed that cyberspace is a domain of operations in which NATO must defend itself, akin to its previous remit to do so in the air, land and sea.[542] NATO Secretary General Jens Stoltenberg has confirmed that a cyber attack can trigger Article Five,[543] NATOs principle of collective defence.[544] While Article Five has yet to be triggered in response to a cyber attack, NATO is still a provider of security to some degree of UK CNI: by extending the notion of collective defence to the cyber domain, potential aggressors may be deterred to attack UK CNI. It should also be noted that NATO has an additional responsibility to protect its own networks.[545] However, this does not relate as directly to the protection of UK CNI.

The UK government is also one of the sponsoring nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Although the CCDCOE's primary mission is research and analysis (akin to a military think tank), the centre also organises an annual crisis simulation exercise called 'Locked Shields.'[546] The 2016 event included teams from NATO members including the UK and the event itself is organised by a number of organisations including the British Army.[547] The 2016 event simulated an attack on an industrial control system that the national teams had to defend against.[548]

[542] "Cyber Defence," NATO, February 17, 2017, http://www.nato.int/cps/en/natohq/topics_78170.htm.
[543] Jens Stoltenberg, "Press Conference by NATO Secretary General Jens Stoltenberg Following the North Atlantic Council Meeting at the Level of NATO Defence Ministers." NATO, June 14, 2016, http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.
[544] "Collective Defence - Article 5," NATO, March 22, 2017, http://www.nato.int/cps/en/natohq/topics_110496.htm.
[545] "Cyber Defence," NATO, February 17, 2017, http://www.nato.int/cps/en/natohq/topics_78170.htm.
[546] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."
[547] "Exercise Locked Shields 2016 Highlights Priorities in Cyber Defence," *NATO CCDCOE*, April 21, 2016, https://ccdcoe.org/exercise-locked-shields-2016-highlights-priorities-cyber-defence.html.
[548] ibid.

The European Union Agency for Network and Information Security (ENISA) is a centre for expertise for cyber security in Europe. While one of ENISA's main roles is to protect EU institutions themselves, the agency also works on the issue of CNI. Within its policy remit, ENISA supports member states on the issues of cyber crisis management[549] – an issue that as previously argued is inextricably linked to the protection of CNI. ENISA runs various initiatives to help states, including the UK, to protect their CNI including: providing a range of training days;[550] the hosting of crisis simulation exercises[551] (that typically simulate attacks on CNI); reviews of member state crisis plans and structures; the provision of various studies and publications; and running international conferences that facilitate shared ideas among member states.[552]

In addition to these multilateral efforts, the UK government also cooperates on the issue of protecting CNI with other states on a bilateral basis. The extent of cooperation is closest within the US-UK relationship who have historically enjoyed a remarkably close relationship on the issue of signals intelligence and cyber security.[553] Amongst other cooperative agreements, the UK and US have agreed to cooperate specifically on the issue of CNI protection. In January 2015, during an Obama-Cameron state visit, both governments agreed to bolster their efforts to 'increase threat information sharing and conduct joint cybersecurity and network defence exercises to enhance our combined ability to respond to malicious cyber activity.[554] There was

[549] "National-Level Cyber Crisis Management," ENISA, accessed October 11, 2017, https://www.enisa.europa.eu/topics/cyber-crisis-management/national-level-cyber-crisis-management?tab=details.
[550] "Trainings," ENISA, accessed October 11, 2017, https://www.enisa.europa.eu/topics/cyber-crisis-management/trainings.
[551] "Cyber Exercises," ENISA, accessed October 11, 2017, https://www.enisa.europa.eu/topics/cyber-exercises.
[552] "International Conferences," accessed October 18, 2017, https://www.enisa.europa.eu/topics/cyber-crisis-management/international-conference-series.
[553] Aldrich, *GCHQ*; Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*.
[554] "Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation," *Obama Whitehouse Archive*, January 16, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

also a declared effort to promote and align cyber security best practices and standards that relate to CNI.[555]

Cooperation on an issue as sensitive as CNI is likely to be restricted to key allies only. Indeed, much of such cooperation with other states likely remains confidential and within frameworks such as the Five Eyes intelligence alliance comprising Australia, Canada, New Zealand and the US in addition to the UK. However, bilateral agreements with other states have indicated a degree of CNI cooperation, albeit to a lesser degree. For example, India and the UK have entered into a framework for the UK-India Cyber relationship in November 2015 which included the signing of a memorandum of understanding between national CERTs.[556]

In a similar manner to the range of government actors that protect UK CNI, there are also other international actors that are not tasked directly with the protection of CNI, yet the issue is likely to overlap with their primary remit. For example, EUROPOL, the European Police Office predominantly tackles the issue of cybercrime when it comes to cyber security, yet their purview inevitably expands to include CNI (when trying to prevent terrorist activity for example).

The technical capability of international stakeholder is mixed. Some of these actors have certainly developed a significant capability that can make a meaningful contribution in confronting contemporary cyber security challenges. For example, the CERT network is a critical part of cyber crisis management and respected by many within the technical community. Bilateral ties between the UK and close allies are also used effectively.[557] For example, the UK-US cyber security relationship is strengthened because of the historic

[555] ibid.
[556] "UK-India Defence and International Security Partnership," GOV UK, November 12, 2015, https://www.gov.uk/government/news/uk-india-defence-and-international-security-partnership.
[557] Interview with William Harvey.

relationship between the two countries' intelligence communities.[558] Yet, many international actors have failed to develop a meaningful material capability. NATO, for example, has been tasked with only protecting its own networks – it has not developed a capability to provide cyber security at a larger scale. Likewise, the NATO CCDCOE relies on member countries sending non-cyber-specialists, often on temporary secondments. This means that the organisation has struggled to develop long-term human capital with deep skills on the issue of cyber security.[559]

Academic Actors

Within academia, there is a great deal of expertise, or human capital, related to various aspects of the cyber security of CNI. This is illustrated through the range of academic centres looking at the issue. This insight ranges from highly technical matters to those that are more political or strategic in nature. Further, 25 masters degrees and two bachelor's degrees in cyber security are currently certified by NCSC, reflecting the scale of training and expertise that exists within academia.[560] Yet, in other forms of capital, academic actors enjoy less power. Although cyber security is an emerging topic in academia, there is still not anywhere near the amount of money available to spend when compared to private actors. Likewise, academic actors do not own portions of UK CNI directly.

The UK Cyber Security Strategy was keen to emphasise that academia plays a key role in the UK cyber security strategy.[561] The PETRAS Internet of Things (IoT) Research Hub is a consortium of nine leading UK universities which will work together over the next three years

[558] Aldrich, *GCHQ*.
[559] Based on the author's own experience working as a project researcher at the NATO CCDCOE.
[560] "NCSC-Certified Degrees," NCSC, August 9, 2017, https://www.ncsc.gov.uk/information/ncsc-certified-degrees.
[561] "National Cyber Security Strategy 2016-2021," HM Government.

to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security.[562] Here, 'National and International Policy for Critical Infrastructure Cybersecurity' is one of the core themes of the research hub. The research group, comprised of academics from various universities will compare and contrast approaches to managing IoT threats from a policy perspective with the threat against CNI recognised to be growing and increasingly severe.[563] The research group will examine policies from a range of key UK stakeholders from smaller companies to multinationals.[564] It will then be considered how this aligns with governmental policy, before contrasting this to similar efforts in Europe and further internationally.[565] A range of UK CNI actors are official partners with the research group including Network Rail, Highways England, CPNI and BT.[566] In addition to the PETRAS hub, a number of research groups and academics have examined the cyber security of critical national infrastructure from various disciplines and areas of focus.

Here, academics are largely incentivised by their own interests related to highlighting, examining and solving questions related to the cyber security of CNI. Academics and academic centres are also dependent on funding and thus incentives to produce research and research proposals that attracts funding. Research may therefore be influenced by funding calls and the interests of funders.

***

Having outlined the various cyber security actors, it is immediately apparent that state-centric paradigms are limited in their ability to reflect the empirical reality of CNI cyber security

[562] "About," Petras, accessed October 11, 2017, https://www.petrashub.org/about/.
[563] "National and International Policy for Critical Infrastructure Cybersecurity," PETRAS, accessed October 11, 2017, https://www.petrashub.org/portfolio-item/national-and-international-policy-for-critical-infrastructure-cybersecurity/.
[564] ibid.
[565] ibid.
[566] ibid.

provision in the UK. This is most apparent given that the government actors are not necessarily the largest or main provider of cyber security. Instead, government actors operate in a more crowded assemblage that comprises corporations (that own approximately eighty percent of UK CNI)[567] as well as both international actors and academic actors (the latter albeit playing a more limited role in security provision specifically). Furthermore, even within 'the government', there are various entities providing cyber security to UK CNI in some capacity, leading to questions regarding the coherence of the government as a single unified actor.

Within the UK CNI cyber security assemblage, the majority of actors have an incentive to improve the cyber security of CNI. In this regard, there are few, if any, instances of alternative forms of security clashing or disagreements regarding the desired outcome – no security actor has a substantive interest in the cyber security of CNI being highly vulnerable or exposed (except arguably those that assist with cyber crisis management and incident response). Yet, despite the vast majority of security actors hoping to improve cyber security, there remain clear divergences in relation to the extent to which security actors are trying to achieve this outcome. These divergences are often caused due to the prioritisation of other objectives – a private sector firm may prioritise low costs over investments in cyber security for example. For government and many international actors, the development of a cyber security presence may be in part incentivised by a desire to grow as an institution. Although having a variety of security actors trying to improve the cyber security of CNI should be welcomed, the competition for mandate between actors also leads to the duplication of functions, often in an unnecessary and inefficient manner.[568]

[567] Ashford, "Is UK Critical National Infrastructure Properly Protected?"
[568] Interview with Cabinet Office employee by the author. Phone. June 9, 2015.

Assemblage Dynamics: the competition of security provision and entrenched partnership structures

The key traits of the UK CNI Assemblage Configuration outlined above make for what is broadly a harmonious structure with significant levels of fusion between corporations and UK Government actors. Such a dynamic has come about given a lack of clashing securities or severe disagreements between security providers. Different security providers have also recognised the mutual benefit in entering into partnership agreements (although these arrangements often contain dysfunctional elements as the following analysis will show).

Despite the broad level of harmony, and with significant aspects of fusion, the UK CNI Assemblage does nonetheless contain two aspects of tension related to disagreement between what elements of security provision belong in the public or private sphere, and through intra-governmental rivalry. However, the current assemblage structure is unlikely to change significantly – both due to the entrenched nature of public-private partnerships (that now make it difficult for the UK Government to significantly challenge the role of corporations) and given that various intergovernmental rivalries have now been settled (through the creation of the NCSC that has made significant progress in clarifying and solidifying the distribution of the cyber security remit within the UK Government).

Internal Workings of the UK CNI Assemblage

The vast majority of the cyber security of UK CNI is provided by a domestic public-private inter-unit cluster that exists between corporations and UK Government actors – the two most prominent security providers within the assemblage. While both of these traditional units – and the specific actors that sit within them – might provide security in independent capacities, they

often work together through partnerships. This partnership is the most prevalent inter-unit cluster, yet one where corporations enjoy a significant degree of power and control. The encompassing nature of this inter-unit cluster means that it therefore forms the majority of the analysis in the following sections of this chapter.

One clear area where government-corporation fusion exists is through information sharing agreements that are one of the most emphasised practices of UK the public-private partnership cluster.[569] Public and private UK CNI security actors share three categories of information. First, they share threat intelligence related to the methods that aggressors use. This includes how aggressors seek to breach systems, what they seek to do once they have breached a system. On a more technical level, specific malware will also be shared. Organisations will also share aggressors IP addresses so that other organisations can know when activity is originating from a likely malicious source. Second, security actors share information regarding exploits and vulnerabilities.[570] Third, security actors share information regarding security protocols. This might include sharing instances of best practice – for example, in the event that an organisation has enjoyed particular success in.

UK CNI security providers share information in the above three categories through a number of forums. The most notable public-private arrangement in the UK is the Cyber Information Sharing Partnership (CISP) launched by CERT-UK in 2013 and now part of the NCSC. The CISP is a joint public-private initiative established to share threat information in real time. Members of the partnership receive threat and vulnerability information from the 'Fusion Cell', a joint industry and government analytical team who examine, analyse and feedback cyber information from a wide variety of data sources.[571] As of May 2016, over 2225 organisations

[569] Carr, "Public–Private Partnerships in National Cyber-Security Strategies," pp. 57.
[570] For example, in March 2016, GCHQ discovered security loopholes in a new UK nationwide system of smart energy meters. See, Pilita Clark, "GCHQ Intervenes to Secure Smart Meters Against Hackers."
[571] *"Cyber Security Information Sharing Partnership (CISP)," NCSC, September 27, 2016.*

and 6150 individuals have signed up to the free service.[572] By embedding both corporations and government actors into such hybrid institutions, public-private distinctions become altogether more blurry.

In addition to the CISP, other smaller information sharing initiatives exist outside of the domestic public-private cluster. For example, ENISA facilitates information sharing at the European level. The UK government also has set up information sharing partnerships with varying degrees of sharing between other governments such as the US and India.[573] It is also possible and indeed likely that information is shared between intelligence agencies such as through Five Eyes (although details of this are not publicly available).

Cyber simulation exercises also bring different stakeholders together – used by organisations to prepare for future attacks and crisis situations, typically though a staged cyber attack. Exercises can range from technical to high-level and increasingly comprise a variety of challenges that test different sections of an organisation. For example, an exercise might simultaneously include a technical challenge for security teams, media and customer communications challenges for press relations teams and questions regarding business management and resource allocation for senior leaders organisations often use cyber simulation exercises as a means for gauging their internal preparedness; yet they are also a crucial way that different organisations are brought together through collaborative, multi-player simulation exercises.

The most advanced sector to engage in multi-stakeholder simulation exercises is the financial sector that has run a long-running series of cyber exercises[574] that are part of a wider collective

[572] ibid.
[573] "UK-India Defence and International Security Partnership."
[574] These include the Market Wide Exercise (2011), Waking Shark I (2011), Waking Shark II (2013), and Operation Resilient Shield (2015).

exercising partnership between public and private actors.[575] One of the most sophisticated of these was Waking Shark II that took place in 2013. A Bank of England Report on the exercise stated that approximately 220 people attended the event with participants including fourteen firms, six financial market infrastructure providers, the Financial Authorities, Bank of England (including the Prudential Regulation Authority), Financial Conduct Authority, HM Treasury, and other government actors.[576] Information sharing via the CISP platform was a particular focus of the exercise and the takeaways of the event were used to identify areas of improvement for the information sharing process.[577] Since Waking Shark II, the scope of simulation exercises has increased within the financial sector. The UK collaborated with US authorities to run a banking industry resilience exercise called Operation Resilient Shield in 2015 that was designed to facilitate an exchange of domestic best practices between the two countries. Several leading global finical firms were involved[578] as well as a range of government actors from both the UK[579] and the US.[580] Rather than testing the cyber security of individual private firms or financial systems more broadly, the exercise was designed to improve understanding across public and private actors in three main areas: information sharing, incident response handling, and public communication.[581]

---

[575] Chris Keeling, "Waking Shark II: Desktop Cyber Exercise Report to Participants," (London, UK: British Banker's Association, November 12, 2013) pp. 2.
[576] ibid., 3.
[577] For example, CPNI struggled to manage their information sharing platform given that their were multiple threads running through the exercise. It was also noted that there was no central industry coordination body for financial sector information sharing and communication to the wider public. See ibid., 2.
[578] John Leyden, "UK Joins US Financial Institutions for Industry Resilience Tests," The Register, November 19, 2015, https://www.theregister.co.uk/2015/11/19/resilient_shield/.
[579] Participants from the UK included CERT-UK, the UK Financial Authorities (HM Treasury, the Bank of England and the Financial Conduct Authority), Cabinet Office, the National Crime Agency, the Office of Cyber Security & Information Assurance and UK Intelligence. See, "Transatlantic Exercise to Tackle Cyber Threat," GOV UK, November 12, 2015, https://www.gov.uk/government/news/transatlantic-exercise-to-tackle-cyber-threat.
[580] Participants from the US included the White House National Security Council, the Department of the Treasury, the Department of Homeland Security, the Federal Bureau of Investigation, the US Secret Service, the Board of Governors of the Federal Reserve System, the Federal Reserve Bank of New York, Federal Reserve Bank of Chicago, U.S. Intelligence Community, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, U.S. Securities and Exchange Commission, U.S. Commodity Futures Trading Commission, and the National Credit Union Administration. See ibid.
[581] ibid.

The US and UK have also worked together in setting up cyber exercises for nuclear plants. In 2016 the US and UK staged a war-game that stimulated a cyber attack on a nuclear power plant, designed to test the readiness of the government and utility firms.[582] In a separate exercise, UK defence contract QinetiQ hosted a simulation of an online terror attack on the nuclear industry. Here, contestants were amateurs rather than established public and private actors – the intention of the exercise being to promote and attract those with technical skills to pursuing a career in cyber security.[583]

As discussed previously in the overview of international actors, both the NATO CCDCOE and ENISA run simulation exercises between government actors. ENISA manages Cyber Europe, a programme of pan-European exercises that occur every other year. Cyber Europe is a series of EU-level cyber incident and crisis management exceed uses for both the public and private sectors from the EU and EFTA Member States.[584] NATO CCDCOE organises an annual crisis simulation exercise called 'Locked Shields' that includes participation from the UK army.[585]

It is therefore clear that corporations and the UK Government work closely together, often to the point that hybrid entities emerge (such as the CISP). Further, in addition to simulation excises and information sharing agreements, that mutually bring actors together through new initiatives, both corporations and UK Government actors are increasingly welcoming the other unit into what has traditionally been regarded as their own spheres – thereby further increasing hybridity.

[582] Heather Stewart, "UK and US to Simulate Cyber-Attack on Nuclear Plants to Test Resilience," The Guardian, March 30, 2016, https://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience.
[583] Ava Fedorov, "Simulation Exercise Tests UK Response to Cyber-Terrorism," SC Magazine, January 27, 2015, https://www.scmagazineuk.com/simulation-exercise-tests-uk-response-cyber-terrorism/article/1478940.
[584] "Cyber Europe," ENISA, April 26, 2017, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.
[585] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."; "Exercise Locked Shields 2016 Highlights Priorities in Cyber Defence."

The UK Government brings corporations into its remit through outsourcing. While the majority of UK CNI has already been privatised, those assets that are under government control still contain interaction with private actors through outsourcing. Outsourcing is a vital component of UK security strategy. For example, the 2015 National Security Strategy and Strategic Defence and Security Review document states that the government will 'continue to reform the MOD to make it leaner and more efficient, outsourcing key functions where the private sector can deliver better, and investing in skills for the roles we retain' while simultaneously announcing a 30% reduction of civilian employees at the MOD.[586] Given a faith in outsourcing in security strategy more broadly, outsourcing therefore naturally forms a fundamental tenet of the UK cyber security strategy beyond just the protection of UK CNI. As of May 2017, the UK government had posted 4306 government contracts with 'cyber security' in the title.[587] 1000 cyber security government contracts have been awarded.[588] In March 2010, GCHQ along with contractors purchased a new £40m site in Cheltenham to house its contractor staff[589] (suggesting that GCHQ envisages that outscoring will remain a key part of their organisational strategy in the long-term).[590] The scale of government cyber security outsourcing is also apparent through the Cyber Growth Partnership, a joint industry and Government group with an emphasis on increasing exports. The partnership allows UK government cyber security suppliers to reference their work for the UK government publicly for the purposes of pursing business overseas. The partnership includes over 563 organisations, including a number of large cyber security consultancies.[591] Given the sensitivity and security concerns of UK CNI, details of outsourcing arrangements for government owned CNI are often kept confidential.

[586] "National Security Strategy and Strategic Defence and Security Review 2015," 33.
[587] "Contracts Finder," GOV UK, accessed March 12, 2017, https://www.contractsfinder.service.gov.uk/Search/Results.
[588] ibid.
[589] "Intelligence and Security Committee Annual Report 2010–2011," (London, UK: HM Government, 2011).
[590] It should be noted that contractors are used for both cyber security and intelligence gathering. A more precise breakdown of the balance between the two is unavailable.
[591] "Registered UK Organisations," Cyber Exchange, accessed October 25, 2017, https://cyberexchange.uk.net/#/directory.

The most fundamental CNI government assets, such as the NHS, and the emergency and security services, have been excluded from the scheme.

Likewise, UK Government actors have become increasingly embedded in the traditional functions of private CNI functions by playing a supportive function to private owners of CNI. The UK government takes a special interest in privately owned CNI assets. Both GCHQ and the CPNI perform risk assessments and audit security arrangements for UK CNI actors.[592] The CPNI has also made twenty specific control recommendations for owners of CNI to implement.[593] The CPNI also provides advice to both public and private CNI firms in areas that may pose a security concern including the Internet of Things and Industrial Control Systems,[594] insider threats,[595] and supply chains.[596] It should be emphasised that much of the recommendations and auditing remains at a high-level, reflecting that the government has so far operated in a largely hands-off capacity in terms of prescribing security protocol.[597] For example, while CERT-UK (now part of the NCSC) does have technical staff and expertise that can be offered to government departments, use of this capability is reserved for severe emergencies on the theory that departments will normally be able to address problems themselves.[598] Part of this reflects the specific challenge of securing CNI (such as securing idiosyncratic legacy systems). The bespoke nature of the infrastructure means that at the technical or detailed level, it is typically the owners and staff of that infrastructure that

[592] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."
[593] Harrop and Matteson, "Cyber Resilience: A Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA."
[594] "Internet of Things and Industrial Control Systems," CPNI, accessed April 27, 2017, https://www.cpni.gov.uk/internet-things-and-industrial-control-systems.
[595] "Cyber Insider," CPNI, accessed April 27, 2017, https://www.cpni.gov.uk/insider-threat.
[596] "Supply Chain," CPNI, accessed April 27, 2017, https://www.cpni.gov.uk/supply-chain.
[597] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom."
[598] ibid.

understand it best – whilst cyber security government actors' ability to provide recommendations is more limited.

Despite the blurring distinctions between the UK Government and CNI corporations, CNI corporations remain in many instances the dominant group given their capabilities and prominence. As previously mentioned, around 80% of UK CNI is privately owned. What is striking here is not just the degree of private ownership but the extent of private governance. Indeed, there is an absence of any central point of control or laws requiring operators of CNI conform to minimum security standards[599] This has meant that government actors have largely treated the owners of CNI as responsible for managing cyber attacks against their own systems.[600] UK government actors have therefore largely played a hands-off role in mandating or controlling CNI corporations. When government actors have intervened previously, their involvement has been in a supporting or coordination role. This has included the provision of auditing and risk assessments, as well as the introduction of certification schemes including Cyber Essentials and Cyber Essentials Plus. This hands-off role has occurred as UK Government actors have recognised that private corporations possess a great deal of the material power and that a government contribution is therefore best served at a higher level in a coordination capacity. There is an acknowledgement that CNI exists in a variety of sectors that need to be managed differently given the specific challenges faced in particular industries and the highly-specialised nature of the technology used.

Yet the growth of government actors' cyber capability over time has been accompanied by a more assertive stance. The extent to which cyber security should be provided by corporations has been directly challenged at an ideational level. The 2016 UK cyber security strategy has

[599] Interview with William Harvey; Ashford, "Is UK Critical National Infrastructure Properly Protected?"
[600] Carr, "Public–Private Partnerships in National Cyber-Security Strategies;" Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."

also signalled that a change of emphasis is required, with more direct government intervention required (this shift in official strategy will be explored further in the second example case below).

Corporations are also set to be faced with further regulatory challenges, most clearly seen in an EU context through the General Data Protection Regulation (GDPR) that comes into force in May 2018 and will be upheld in spirit within the UK despite the outcome of UK negotiations in terms of leaving the EU. The GDPR will require businesses to notify both customers and authorities about data breaches and egregious violation of the cyber security requirements in the regulation could lead to fines up to either 20 million euros or four percent of revenues – whichever is highest.[601]

Similar to the dynamics of the domestic public-private inter-unit cluster outlined above, the dynamic within the UK Government also contains elements of contradiction. Again, there are no direct and incompatible views of security with all government actors hoping to secure CNI infrastructure. Yet, there remains a level of rivalry and competition between the different government actors.[602] Much of this stems from the highly decentralised approach that the UK Government has taken with a range of government actors providing cyber security to UK CNI in some form. The Cabinet Office has been cautious about escalating too many powers and responsibilities up to the Prime Minister and central government departments. The 2011 Cyber Security Strategy document stated that government responsibilities for CNI and crisis situations should be 'provisional and can be adjusted if experience suggests that a different mix of inputs will produce better results.'[603] Responsibility for CNI and cyber crisis situations has

[601] Stephen Cobb, "Is the World Ready for GDPR? Privacy and Cybersecurity Impacts Are Far-Reaching," We Live Security, May 23, 2017, https://www.welivesecurity.com/2017/05/23/gdpr-is-world-ready-cybersecurity-impact/.
[602] Interview with cyber security consultant (a); Interview with cyber security consultant (b) by the author. London, UK. May 21, 2015.
[603] "The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World."

therefore lied with relevant government departments (i.e. The Department of Health is responsible for securing government health assets and overseeing private health firms). This decentralised approach has the advantages of facilitating a formalised, yet flexible approach: the government can bring in different departments as and when a situation requires.[604]

Despite the thinking behind such a decentralised approach, the position taken has led to inefficiency and created tension within the UK Government. A 2015 UK security strategy review acknowledges this reality, stating that 'responsibilities for infrastructure policing are shared across several organisations with different levels of capability and capacity, and different arrangements for funding, oversight, regulation and legislation.'[605] While such a setup provides a highly flexible approach to responding to serious attack on UK CNI,[606] it also leads to a highly complex configuration of actors, making for a 'patchwork quilt' of responsibilities amongst the various government actors.[607] When the variety of departments, and their divergent incentive structures are considered, it is clear that there is not a coherent unified government entity operating in the context of CNI. Instead, aspects of the government landscape are characterised by competition between government entities. Various interviewees working within Government stated, that the decentralised approach has led to the protection of UK CNI becoming overcrowded with too many government institutions involved.[608] As James Snook, Deputy Director of the Office for Cyber Security and Information Assurance, acknowledged, within government there is 'an emerging alphabet soup of organisations doing various things on cyber.'[609] Inevitably, there is overlap between different departments leading

[604] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."
[605] "National Security Strategy and Strategic Defence and Security Review 2015," 44.
[606] Collier, "Strategies of Cyber Crisis Management: Lessons From the Approaches of Estonia and the United Kingdom."
[607] Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," 1098.
[608] Interview with Cabinet Office employee; Interview with William Harvey.
[609] Talal Rajab, "Briefing with James Snook on National Cyber Security Strategy," techUK, June 21, 2016, https://www.techuk.org/insights/meeting-notes/item/8704-briefing-with-james-snook-on-national-cyber-security-strategy.

to inefficiency. An example of this was explained by one interviewee working for the Cabinet Office who explained that both Her Majesty's Revenue and Customs (HMRC) and the Department for Work and Pensions (DWP) run their own security operation centres, despite such a facility also being provided by GCHQ and the NCSC.[610] Crucially, however, a devolved approach fosters dysfunctional relationships between departments. Government departments are not necessarily incentivised to cooperate with one another. Two interviewees that advise and consult with UK Government actors claimed that much of the problem stems from each department seeing itself as sovereign and therefore prioritising its own survival and growth on a stand-alone basis over that of the collective UK Government. Different departments are potentially faced with conflicting objectives. It is reported that cultural gaps exist between organisations that seek to prevent cyber-attacks (e.g. law enforcement) and those that exist to respond to cyber attacks and minimise the damage (e.g. CERT-UK).[611] Various government actors seek to develop their own cyber security presence given that such a remit enables them to grow as an entity. This has meant that the various government departments have been, at times, reluctant to cooperate.

While each government actor has a different function, there is inevitably overlap and at times inefficiency in such a crowded space. Ultimately, with so many government organisations looking at the issue, it is impossible to see the government as a coherent whole in this space. Although various government entities recognise the importance of cyber security, competing objectives often take precedent. This is particularly pertinent in the UK given the Conservative led governments have introduced austerity policies, with most government budgets being cut. Without delving into normative arguments regarding these policies, cutbacks have inevitably left government departments more strained. Often here, the priority has been to maintain

[610] ibid.
[611] Tracey Caldwell, "Call the Digital Fire Brigade," *Network Security* 2014, no. 3 (March 14, 2014): 5–8.

current services or at least mitigate the impact of budget cuts. New initiatives or those related to technology and cyber security are often not seen as a priority. In such a resource-constrained environment, the impact of not following cyber security advice may not be foreseen. In these instances, and faced with many pressing concerns, delaying investment in often costly, time consuming and uncertain cyber security investments may seem a rational decision.[612] Further, while specific government budgets have been cut, government cyber security spending has increased to £1.9 billion of spending pledged between 2016 and 2021. Here, several government actors compete for different parts of the cyber security mission.

Just as there has been rivalry between domestic government actors, it is also clear that various international organisations have begun to develop themselves as cyber security bodies. While there is not the same extent of competition between these organisations, each actor has nonetheless sought to frame cyber security as an issue that suits their own interests. NATO has framed the issue as the 'fifth domain of warfare' while the EU has framed cyber security in relation to issues such as the Digital Single Market' for example.[613] Here, there is overlap between the cyber security functions – both the EU and NATO host similar cyber crisis simulation exercises for example. Both compete to frame cyber security issues in particular ways (NATO, for instance, has sought to largely militarise cyber security through discussion the issue in a military context). This would suggest that international actors compete for the cyber security remit, as the issue has increased in importance. Of course, the motivations for international actors is not just expanding remits: they also genuinely hope to contribute to solving cyber security challenges.

[612] Collier and Martin, *Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand.*
[613] Jamie Collier, "Written Evidence Submitted to the Joint Committee on Cyber Security: Critical National Infrastructure Inquiry," February 13, 2018, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/written/76828.pdf.

Yet, despite the emerging profile of these international organisations, two interviewees working for the UK Government explained that it is often more traditional cyber security cooperation mechanisms that are favoured – including the FIRST network of CERTS, Five Eyes discussions, and even bilateral discussions with the states where an attack is emanating or with previous victims of such an attack.[614]

Evolution: from market forces to market failure

When considering the evolution on the UK CNI Assemblage, it would appear that many of the tensions, where they have existed, now appear to be at least partially settled. As discussed in the previous section, the domestic public-private cluster faces a contradiction: while the UK Government has contested the role of corporations and the ability of a market-driven approach to deliver the required cyber security investment, it remains in a deep partnership with them. It is this partnership entrenchment that represents a source of stability, making it significantly more difficult for official UK Government strategy to significantly change emphasis by challenging the role of corporations.

The stability of the assemblage looked to be disrupted through the publication of the UK Government 2016 Cyber Security Strategy[615] and various public statements that preceded it[616] (discussed in greater detail in the second example case below) that emphasised a more assertive and sceptical tone from official UK Government cyber security strategy in its posture towards private sector security with it being made clear that the private market has not functioned as was envisioned in 2011.

[614] Interview with William Harvey.
[615] "National Cyber Security Strategy 2016-2021."
[616] For example, see Reeve, "Industry's Cyber-Security "Market Failure" Must Be Addressed,"; Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," Financial Times.

Yet, despite the official UK Government's position to publicly challenge the role of corporations, it is unclear whether this will lead to material and political shifts in practice. As academics such as Carr have highlighted, government actors are reluctant to take on further action as this would also involve absorbing a greater portion of the responsibility and therefore blame in the event of a serious cyber attack.[617] In many respects the 2016 cyber security strategy represented a change in rhetoric rather than substance with the document still heavily emphasising the importance of UK Government partnerships with corporations.[618] An interview with a chief information security officer at one large CNI organisation confirmed this much, with it suggested that UK Government actors might become more involved in suggesting how CNI organisations can make investments, while not compelling them to take certain courses of action (thereby remaining in a hands-off and advisory capacity).[619] There is also evidence that suggests government actors will intervene only lightly. In a speech at GCHQ, the then Chancellor George Osbourne stated that 'new regulation will need to be carefully done – light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it,' indicating that the government is cautious about over-regulating in this space.[620] Former GCHQ Director Robert Hannigan stopped short of calling for new laws in his speech on the topic.[621] Apart from the introduction of GDPR, government interventions has occurred in altogether lighter ways . There has also been a noticeable absence of government discussion regarding the shifting of liabilities to make UK CNI firms more liable for the damage caused by security breaches. Government actors are looking at ways to encourage, rather than force, cultural change. For example, UK cyber security officials are

[617] Carr, "Public–Private Partnerships in National Cyber-Security Strategies."
[618] Government, "National Cyber Security Strategy 2016-2021."
[619] Interview with Chief Information Security Officer of a UK CNI Organisation by the author. London, UK. October 6, 2015..
[620] Osbourne, "Chancellor's Speech to GCHQ on Cyber Security."
[621] Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," Financial Times.

looking to Israel[622] as an example of a state that has a well-developed private cyber security sector that is nurtured by the Israeli government and its intelligence agencies.[623] It may be that government intervention is felt through the creation of further accreditation schemes and standards, rather than more explicit regulation. Crucially, the harder line promised by the 2016 strategy has not translated into action in either 2017 or 2018.

Of course, the public-private nexus could still shift if the UK Government introduces regulation at a later date (although there is no indication that a tougher approach will be introduced). It also remains to be seen exactly how GDPR regulation will be interpreted and whether the maximum fines possible will be imposed on private owners of CNI. Further, the rising popularity of the leader of the opposition, Jeremy Corbyn who has campaigned on a platform to renationalise aspects of CNI[624] – alongside polling data that shows the falling popularity of privatisation of CNI[625] – shows that there is emerging political support for stricter controls of CNI firms. If not nationalisation, this could also involve stricter regulation with cyber security being an obvious area to that would receive scrutiny given the previous assessments outlined above within official government strategy documents. Likewise, Prime Minister May has shown a greater scepticism of (whilst not completely dismissing) further Chinese investment in CNI for example,[626] thereby suggesting a cautious political strategy in regard to welcoming foreign corporations.

---

[622] ibid.
[623] John Reed, "Unit 8200: Israel's Cyber Spy Agency," Financial Times, July 12, 2015, https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c.
[624] Asthana and Stewart, "Labour Party's Plan to Nationalise Mail, Rail and Energy Firms," The Guardian.
[625] Smith, "Nationalisation vs Privatisation: the Public View."
[626] Terry Macalister, "Hinkley Point C: No Easy Solution to Theresa May's Chinese Puzzle," The Guardian, September 3, 2016, https://www.theguardian.com/uk-news/2016/sep/03/hinkley-point-c-theresa-may-china-g20-summit; Steven Swinford and Emily Gosden, "Theresa May Delays Hinkley Nuclear Decision Amid Concerns Over Chinese Involvement," The Telegraph, July 29, 2016, http://www.telegraph.co.uk/business/2016/07/29/theresa-may-delays-hinkley-nuclear-decision-amid-concerns-over-c/; Andrew Ward, Jim Pickard, and Michael Stothard, "Hinkley Go-Ahead After 'National Security' Safeguards," Financial Times, September 15, 2016, https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43.

Similar to disputes related to the public-private nexus, the extent of departmental rivalry in the UK CNI Assemblage looks to become increasingly stable going forward. Whilst cyber security capability has previously been distributed amongst a variety of government actors (and will continue to do so), large elements of the UK Government's capability have nonetheless been centralised through the creation of the NCSC. When announcing the intention to build the Centre, the then Chancellor Osbourne claimed that 'the Centre will be a unified source of advice and support for the economy, replacing the current array of bodies with a single point of contact.' For example, CERT-UK and CESG (the previous cyber security arm of GCHQ) have both been integrated into the NCSC. However, the creation of the centre has not wholly solved the issue with several government departments (as outlined earlier in this chapter) still having a clear stake in the cyber security of UK CNI. The NCSC is also a relatively young organisation (being launched in 2016) and it may be that the NCSC captures a greater portion of the governmental cyber security remit over time. A former GCHQ employee suggested that given the NCSC has a unit concerned with public policy, it may start to challenge the strategic aspects of the Cabinet Office team for example.[627] With the NCSC's mission to establish itself as the central focus of cyber security issues across government entities, it is unlikely that this position will be seriously challenged going forward.

The intergovernmental rivalry was therefore more intense prior to the NCSC when large portions of the cyber security remit were still not formally allocated – leading to competition between different government actors. One interviewee working for the UK Government at the time stated that they campaigned, along with others, for the NCSC to be housed within the Cabinet Office with the argument for doing so seriously considered.[628]

[627] Interview with former Government Communications Headquarters employee by the author. Oxford, UK. September 16, 2016.
[628] Interview with National Cyber Security Centre employee by the author. London, UK. November 23, 2017.

As previously discussed, various international actors are competing for similar cyber security remits. While this could lead to serious shifts and competitions for power, for the purposes of the case study in question, it is not judged to be as significant given that a great deal of the UK response to cyber security does not involve international actors in as significant a capacity. As the internal processes section confirmed, the UK is more likely to stay involved with more traditional cooperation mechanisms. Further, it is likely that the EU's cyber security role in the UK, if anything, will reduce as the UK leaves the EU. The competition between international actors is, however, more relevant in other contexts: with international actors playing a more prominent role in the Estonian cyber security context, the issue of rivalry and competition between international actors will be addressed in further detail in Chapter Five.

Example One: Foreign involvement in the UK CNI Assemblage

It has been argued that corporations are the dominant force within the UK CNI Assemblage and this is exhibited most clearly through the prominent, and often highly controversial, role that foreign-based firms have in developing, maintaining, and securing CNI systems in the UK. Under Prime Minister David Cameron, there was a substantial shift in national strategy to further embrace Chinese investment.[629] This has continued, albeit more cautiously, under Prime Minister Theresa May.[630]

[629] "UK's Unbalanced Relationship with China," Financial Times, September 22, 2015, https://www.ft.com/content/b18ae09c-611c-11e5-9846-de406ccb37f2?mhq5j=e5; George Parker and Elaine Moore, "George Osborne Says UK and China 'Will Stick Together'," Financial Times, September 22, 2015, https://www.ft.com/content/be5c0e8c-607b-11e5-9846-de406ccb37f2; Dan McCrum, "City's Embrace of China Comes with Risks," Financial Times, October 22, 2015, https://www.ft.com/content/6b9fd03e-78d1-11e5-933d-efcdc3c11c89?mhq5j=e5.

[630] For example, Prime Minister May delayed approving the Hinkley Point project amid concerns over Chinese involvement. While the project was eventually approved, plans to tighten screening of foreign investments by China and other countries was proposed in the Conservative party 2017 election manifesto. See, Swinford and Gosden, "Theresa May Delays Hinkley Nuclear Decision Amid Concerns Over Chinese Involvement,"; Macalister, "Hinkley Point C: No Easy Solution to Theresa May's Chinese Puzzle,"; "Forward Together: Our Plan for a Stronger Britain and a Prosperous Future," (The Conservative and Unionist Party Manifesto 2017, May 2017).

Huawei is one of the largest providers of telecommunication equipment in the UK and has deals in place to provide CNI as well as the technology behind services for a number of companies' UK operations including BT, EE, Virgin Media, O2 and Sky.[631] The company, which was founded by a former military technologist from the Chinese army,[632] provides services across all aspects of the telecoms infrastructure chain, including the technical boxes and masts that carry voice and data communications to the software that runs the network and the handsets that receive calls.[633] While the firm is owned and largely controlled by its own employees,[634] there has been scepticism in the West over its alleged ties with the Chinese government.[635] Critics have asserted that Huawei is not truly employee-owned given that its foreign staff cannot join the ownership plan with Chinese domestic law requiring that participants are both employees and Chinese nationals.[636] The concern over ties to the Chinese government have meant other Western states including Australia and the US have barred the Chinese multinational from bidding on national contracts.[637] The UK CNI Assemblage is by contrast more accommodating and open. Rather than barring Huawei, the UK Government has instead introduced mechanisms that enable them to participate in the UK CNI Assemblage (albeit under certain conditions). For example, a cyber security evaluation centre was established by Huawei in Banbury, UK in 2010. At the centre, the physical equipment and

[631] Daniel Thomas, "Huawei Does Not Pose Risk to UK National Security, Report Finds." Financial Times, March 25, 2015. https://www.ft.com/content/70592668-d2e4-11e4-a792-00144feab7de.
[632] Jones and Parker, "GCHQ Seeks to Allay Hinkley Security Fears."
[633] Blitz and Thomas, "Parliamentary Report Raises Alarm Over Lack of Checks on Huawei."
[634] Demetri Sevastopulo, "Huawei Pulls Back the Curtain on Ownership Details," Financial Times, February 27, 2014, https://www.ft.com/content/469bde20-9eaf-11e3-8663-00144feab7de.
[635] Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," (Washington, DC: U.S. House of Representatives, October 8, 2012); Paul Rosenzweig, "The United Kingdom and Huawei," Lawfare, July 25, 2013, https://www.lawfareblog.com/united-kingdom-and-huawei.
[636] Sevastopulo, "Huawei Pulls Back the Curtain on Ownership Details."
[637] Rogers and Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,"; Kathrin Hille, Stephanie Kirchgaessner, and Paul Taylor, "China and the US: Access Denied," Financial Times, April 7, 2011, https://www.ft.com/content/9080ccaa-614d-11e0-ab25-00144feab49a.

software used in the UK is taken apart and inspected by GCHQ employees to mitigate risks to national security - again highlighting the hybrid nature of UK CNI cyber security provision.[638]

Such an accommodating tone has led to controversy. In 2008, MI5 raised concerns over the theoretical potential for the Chinese state to exploit vulnerabilities in Huawei equipment to disrupt UK CNI[639]. A management audit by Ernst & Young assessed that the centre was sufficiently independent from Huawei yet also expressed reservations based on the clearances and vetting procedure of staff as well regarding tensions between teams working in the centre and the Huawei response team in China.[640] The UK parliament's Intelligence and Security Committee also concluded it was "highly unlikely to provide, or to be seen to provide, the required levels of security assurance."[641] Given the sensitivities of such actors with alleged ties to governments, it is difficult to confidently assess the incentive structures of these actors. For the purposes of this thesis, it is assumed that Huawei has a similar incentive structures to most other financially driven multinationals given that the evidence surrounding collusion with the Chinese government over matters of UK national security is either weak or not publicly available at present.

Further, Huawei's role in UK CNI is not an isolated incident, as shown by the foreign involvement in the UK's Hinkley point nuclear plant that is currently in development. As the Assemblage Configuration section discussed, EDF and China General Nuclear Power Corporation are the primary owners of the plant. Like the Huawei case, the involvement of a Chinese entity has been controversial. While Prime Minister May has continued Cameron's strategy of allowing Chinese firms to be involved, it has nonetheless been under a more

[638] Thomas, "Huawei Does Not Pose Risk to UK National Security, Report Finds."
[639] ibid.
[640] ibid.
[641] Sir Malcolm Rifkind, "Intelligence and Security Committee Foreign Involvement in the Critical National Infrastructure: the Implications for National Security Cm 8629," (London, UK: Intelligence and Security Committee, June 3, 2013). pp. 17.

cautious approach.[642] For example, government ministers will be able to prevent EDF from selling its stake in Hinkley.[643] The government will also take a 'golden share' in all future new nuclear project that will ensure that significant stakes cannot be sold without the government's knowledge or consent. On the issue of cyber security specifically, UK government actors will have a hands-on role despite the plant being run by EDF and China General Nuclear Power Corporation. GCHQ will have unfettered access to Chinese computer systems and contractors involved in the project.[644]

The UK National Security Council has raised concerns over the prospect of China being able to build digital loopholes into hardware, allowing Beijing to exploit vulnerabilities at nuclear plants.[645] Nick Timothy, Prime Minister May's former Joint Chief of Staff also expressed reservations over the possibility of China building in weaknesses to computer systems that will allow the Chinese to 'shut down Britain's energy production at will'.[646]

Yet, the UK executive appears broadly confident that dangers will not materialise. As well as holding a trust in GCHQ's ability to prevent such loopholes, there is also a trust in market incentives (that have influenced a great deal of the UK Government approach to CNI) to steer positive Chinese behaviour: Lord Mandelson, former first minister and new president of the Great Britain China centre claimed that 'China knows that should it ever use critical

[642] For example, Prime Minister May delayed approving the Hinkley Point project amid concerns over Chinese involvement. While the project was eventually approved, plans to tighten screening of foreign investments by China and other countries was proposed in the Conservative party 2017 election manifesto. See, Swinford and Gosden, "Theresa May Delays Hinkley Nuclear Decision Amid Concerns Over Chinese Involvement,"; Macalister, "Hinkley Point C: No Easy Solution to Theresa May's Chinese Puzzle,"; "Forward Together: Our Plan for a Stronger Britain and a Prosperous Future," (The Conservative and Unioninst Party Manifesto 2017, May 2017).
[643] "Hinkley Point: UK Approves Nuclear Plant Deal."
[644] Jones and Parker, "GCHQ Seeks to Allay Hinkley Security Fears."
[645] ibid.
[646] Henry Hill, "The Wit and Wisdom of Nick Timothy. 19) Stop Selling Our Security to China," Conservative Home, July 15, 2016, http://www.conservativehome.com/parliament/2016/07/the-wit-and-wisdom-of-nick-timothy-19-stop-selling-our-security-to-china.html.

infrastructure investment as a cover for inappropriate activity, Chinese investment will not be allowed to see the light of day again, anywhere in the West.'[647]

Example Two: shifts in official UK Government cyber security strategy on the role of the market

In addition to the divergent incentives and motivations of actors, there is also conflict in relation to the roles of various actors. This is most clearly seen in current discussions of the public-private nexus. Here, there has been a notable change in rhetoric within official government policy and the stance of government entities in relation to their approach with corporations. UK government actors are currently undergoing a transition in terms of their appetite for government intervention. Central UK government strategy (written by the Cabinet Office and approved by the Prime Minister) has previously advocated a hands-off role in terms of government interference towards private owners of UK CNI. The previous UK government cyber security strategy, published in 2011, proposed a largely hands-off approach by government actors, with an assumption that private firms would be appropriately incentivised to invest in cyber security through market forces alone. The 2011 Cyber Security Strategy stated that 'much of cyberspace is owned and used by private companies. It is businesses that will drive the innovation required to keep pace with security challenges.'[648] The 2011 strategy document also made almost no mention of the need for further regulation[649] with the document instead promoting a public-private partnership model that comprised initiatives that included

[647] ibid.
[648] "The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World," 23.
[649] Regulation is mentioned only twice in the strategy document. The first reference states that 'our sound domestic legal framework and regulatory environment mean that the UK has the basis to respond to cyber crime' while the second reference mentions the UK government's intention to 'undertake a review of policy and regulation of the UK communication sector'. See ibid, p 18, 39.

only voluntary involvement from the private sector (such as through information sharing arrangements and simulation exercises).

Since 2011, there has been a noticeable change of emphasis in UK government strategy. A consensus that there is a market failure in cyber security has prompted an increased willingness by government entities to intervene with private firms more directly. When discussing the failures of the market, the then GCHQ Director Robert Hannigan insisted that the government must act to 'make the market work better.' These sentiments were then repeated by the then Chancellor George Osbourne in a speech at GCHQ who stated that:

> *'Government cannot duck its responsibilities. There are certain things that only government can do, in cyberspace just as in the physical world. Government has a unique ability to aggregate and educate. Only government can legislate and regulate. Only government can collect secret intelligence. Government has a duty to protect the country from hostile attack. Government has a duty to protect its citizens and companies from crime. Only government can defend against the most sophisticated threats, using its sovereign capability. And that's exactly what we will do.'*[650]

The publication of the 2016 Cyber Security Strategy further reinforced the government's modified strategy. The 2016 strategy stated that the previous 2011 strategy document 'achieved important outcomes by looking to the market to drive secure cyber behaviours. But this approach has not achieved the scale and pace of change required to stay ahead of the fast-moving threat. We now need to go further.'[651] Looking forward, the 2016 strategy asserts that

[650] Osbourne, "Chancellor's Speech to GCHQ on Cyber Security."
[651] "National Cyber Security Strategy 2016-2021," H M Government. pp. 9.

'the UK Government intends to intervene more actively.'[652] Given that much of the statements refer to how the government may change and redefine its cyber security role in the future, this issue will be discussed in the following Assemblage Stability subsection.

Although UK government actors have signalled an increased willingness to regulate and intervene in the cyber security practices of private corporations, they have also emphasised the importance of public-private partnerships. Recent government policy should not therefore distract from what is currently a highly harmonious relationship between corporations and government entities. Indeed, the latest UK government cyber security strategy states that investment in 'partnerships with industry and the private sector will continue to underpin our ability to detect, observe and identify this constantly evolving activity against us.[653]

The nature of these public-private partnerships in CNI protection have been rightly criticised by academics. Carr has argued convincingly that in developing partnerships, government actors are relinquished not just authority over the cyber security of CNI but also the responsibility of CNI.[654] The UK 2016 Cyber Security Strategy confirms this much, stating that 'neither the Government nor other public bodies will take on the responsibility to manage this risk for the private sector, which rightly sits with boards, owners and operators.'[655]

Security Outputs: market failure

While CNI systems in the UK are broadly secure – as shown by the lack of public cases of serious disruption – the entities that own and manage CNI nonetheless underinvest in security. This underinvestment has led to an emerging consensus that a cyber security market failure exists (defined as a situation where an individual or businesses' incentives for rational

[652] ibid., pp. 9.
[653] ibid.
[654] Carr, "Public–Private Partnerships in National Cyber-Security Strategies," pp. 44.
[655] Government, "National Cyber Security Strategy 2016-2021."

behaviour does not lead to an optimal outcome for society).[656] This view has been articulated by key UK policymakers as part of the UK Government's challenge (as discussed above). Robert Hannigan, the then Director of GCHQ, stated that 'It is time to take a hard look at whether the international market for cyber security is working sufficiently well . . . something is not quite right here' in 2016.[657] Hannigan went on to argue that the 'global cyber security market is not developing as it needs to: demand is patchy and it is not yet generating supply.'[658] Likewise, James Snook, Deputy Director of the Office for Cyber Security and Information Assurance, has also argued that a market failure in cyber security exists. Speaking about UK private sector firms, Snook claimed that 'with the exception of a few who absolutely do demonstrate best practice and thought leadership in this area, many boards and organisations are not properly managing cyber-risk.'[659]

Several of the variables studied through an assemblage approach in this thesis are relevant for assessing this underinvestment. At the most obvious, is the incentive structures of security providers. Here, while the vast majority of security providers hope for a secure CNI, this is one of many organisational objectives that must be balanced. Security controls can hamper the quality of a product or service (for example, additional security checks may slow down a service or compromise user-friendliness). Implementing cyber security can also slow down the production phase of a product, thereby increasing the time-to-market and reducing profit margins.[660] Firms therefore have an incentive to ship hardware and software as fast as they can and then patch any flaws as and when they are discovered.[661] Although security is certainly

[656] "Market Failure," *Investopedia*, accessed May 9, 2017, http://www.investopedia.com/terms/m/marketfailure.asp.
[657] Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security," Financial Times.
[658] ibid.
[659] Rajab, "Briefing with James Snook on National Cyber Security Strategy."
[660] Kat Hall, "Cybersecurity Is Slowing Down My Business, Say Majority of Chief Execs," The Register, February 17, 2016, https://www.theregister.co.uk/2016/02/17/cyber_security/.
[661] "Not My Problem: Providing Incentives for Good Behaviour," The Economist, July 14, 2014, https://www.economist.com/special-report/2014/07/14/not-my-problem.

considered important, CNI firms often prioritise other aspects such as quality and cost, leading to substantial supply chain risks. Corporations want to ensure secure CNI systems, but strive for this while ensuring their costs are kept low.[662] Government actors may recognise the importance of cyber security but feel they are unable to prioritise the issue given limited resources. Further, CNI organisations often do not bear the full consequences of a serious cyber attack with a significant proportion of the costs passed on directly to individuals.[663] For example, in the event of a cyber attack that results in a power outage, the costs imposed on electricity firms (such as lost revenue and reputational damage) are dwarfed by the overall societal cost (that might include the cessation of critical services and even loss of life).[664] Many UK CNI firms are also monopolies, meaning that consumers would be unable to switch providers in response to a serious cyber security breach.[665] This gap between the intended outcomes in principle and the actual implementation of cyber security has thus led to an incentive deficit.

It is also crucial to understand that underinvestment (or the lack of prioritisation) in cyber security is not restricted to just corporations. Indeed, arguably the most serious cyber incident on UK CNI was the WannaCry worm that devastated NHS systems and led to delays and cancellations. Here, many of the above factors that applied to CNI corporations therefore also apply to public organisations. While they are not profit-seeking organisations, they nonetheless have other objectives. The WannaCry ransomware spread in the NHS provided a case in point with it exploiting outdated software.[666] Whilst running up-to-date software features is routine security advice, in a resource-constrained environment (such as the NHS), the impact of not

[662] Interview with National Grid employee.
[663] Interview with William Harvey; Eli Dourado, "Working Paper: Is There a Cyber Security Market Failure?," *Mercatus Center Working Paper* 12, no. 5 (January 23, 2012): 1–34.
[664] Interview with William Harvey.
[665] Interview with Cabinet Office employee.
[666] Medeiros, "WannaCry Laid Bare the NHS' Outdated IT Network – and It'S Still Causing Problems."

following that advice may not be foreseen. For managers faced with many pressing concerns, a delay to a time-consuming, costly and uncertain update programme may seem a rational decision.[667]

In addition to investment decisions, CNI organisations also face adverse incentives regarding information sharing agreements. Organisations are often reluctant to admit when they have been hacked as disclosures could expose them to litigation or reputational damage.[668] Further, it is often direct competitors that would benefit the most from information shared, meaning it is not necessarily in an organisations' business interests to share information regarding threats and breaches. There is also an entire industry of security firms that sell threat intelligence whose business model would become untenable if they began to provide information free of charge[669] A free-rider problem also exists with organisations happy to benefit from shared information, yet often reluctant to reciprocate themselves.[670] An ENISA report has confirmed this reality, stating that many CERTs (including those in the UK) have shown a 'lack of interest' in sharing information.[671] Many of the organisations that have previously shared information within the UK CNI Assemblage have since given up or reduced their efforts due to this lack of reciprocity.[672]

As well as incentive structures, hybridity and harmony within the public-private partnership inter-unit cluster are also crucial variables in explaining why underinvestment and the security

[667] Collier and Martin, "Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand."
[668] "Not My Problem: Providing Incentives for Good Behaviour."
[669] This includes established vendors who continually gather threat intelligence (including Symantec, McAfee, Trend Micro, FireEye, Sophos, and Kaspersky); suppliers who offer specific threat intelligence gathering, sharing and analysis products, like big data-based security information and event management or network intelligence tools (including Norse, Narus, HP ArcSight, and AlienVault); and wider security platforms where intelligence and analytics comes as part of a broader service offering (including IBM, HP, Verizon, Bluecoat, Orange, and BT).
[670] Interview with National Grid employee.
[671] "Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches," (Athens, Greece: ENISA, December 16, 2015).
[672] ibid., 8.

outcomes discussed have sustained. Crucially, the partnership arrangements between corporations and the UK Government, that have dominated the public-private nexus in the UK CNI Assemblage have become entrenched. The prevalence and reliance on hybrid partnership structures through the practices outlined in the internal process sections (where corporations enjoy significant power and influence) have meant it has been difficult for the UK Government to significantly alter its strategy in practice. This is an interesting, yet largely neglected, dynamic – it might be thought, as observed in the previous chapter, that a highly fragmented and disparate assemblage inherently leads to worse security outcomes precisely because of the rivalry and lack of cooperation between security actors. The UK CNI Assemblage, by contrast, would arguably be more efficient if there was less fusion and more rivalry or fragmentation – thereby allowing the UK Government to intervene and challenge more directly in the affairs of UK CNI corporations. This chapter has therefore highlighted the way in which hybridity is a variable that can also constrain security actors. Of course, the balance between the appropriate level of distance, while still retaining the vital components of partnership arrangements is difficult, if not impossible to fully achieve and inevitably trade-offs exist.

Unlike the US Encryption Assemblage where the opposing views of different security actors acted as a form of check and balance, the higher levels of fusion in the UK CNI Assemblage have actually prevented security actors (and the government in particular) from being able to intervene or confront corporations. In this regard, this chapter has shown how fusion can dissolve what would otherwise be natural checks and balances.

However, even without the current levels of hybridity, the UK Government might still be reluctant to intervene because of its own incentive structures – as Carr has argued, this would require them to take on more responsibility in the event of a crisis situation.[673] With government

[673] Carr, "Public–Private Partnerships in National Cyber-Security Strategies."

actors reluctant to take on greater responsibility over the cyber security of CNI, UK Government documents have typically avoided suggestions of hierarchy when they refer to public-private partnerships as well as avoiding clear statements outlining the division of legal authority, responsibility and rights within CNI sectors.[674] Likewise, with government institutions also motivated by their own growth, cyber security has been seen as a means to an end – a way for government institutions to justify increased budgets.[675] Crucially, the incentive structures of government actors has politicised cyber security budget discussions.

It is also not even clear that government intervention would provide a silver bullet. While UK Government strategy could intervene in the market in numerous ways (such as through setting regulation, mandatory security spending requirements, setting minimum security standards, shifting legal liabilities, etc.), many of these options offer imperfect solutions. Government interventions can simply be ineffective for instance. Whilst setting rudimentary minimum security standards is a useful first step for organisations, they are unlikely to prevent sophisticated threat actors, including sophisticated governmental offensive cyber units. Further, it has previously been argued that encouraging security actors to spend more on cyber security – through either security spending tax credits or mandatory spending requirements – would be unlikely to result in substantially greater security. Instead, it is more likely that existing staff would be nominally reclassified as security personnel and organisations could adjust their accounting to include broader spending on IT equipment as security spending. Ultimately, while such government measures might lead to improvements in security, it could be a highly inefficient process. Government intervention may also have unintended consequences. Regulation and mandatory security requirements raise costs. This increase in costs is likely to be passed onto customers through higher prices that might discourage some

[674] ibid., 62.
[675] Interview with cyber security consultant (a); Interview with cyber security consultant (b) by the author. London, UK. May 21, 2015.

users from consuming a certain product or service.[676] Regulation is also likely to disproportionately harm small businesses and start-ups.[677] This is because larger organisations are more able to comply with security regulation given that they have the resources and personnel to parse and implement new legal requirements. Regulation may therefore have the unintended effect of further increasing the barriers to entry, thereby discouraging start-ups and smaller firms from entering the market. [678]

A further issue that leads to a naturally less secure CNI systems is the complexity that exists within the UK CNI Assemblage. With UK CNI organisations increasingly outsourcing work, cyber security is further undermined. As technology has become more prevalent in CNI, firms are using contractors more than ever given the need to bring in outside expertise and capability in areas such as SCADA systems and cloud services.[679] Contractors compete on a number of fronts including quality, cost and security. More crucially, however, the use of contractors and third parties worsen this incentive deficit – if organisations sell on their hardware and software, they bear a very low proportion of the costs if one of their customers experience a cyber attack as a result of insecure products and services.[680] The variety of actors involved in CNI in the UK makes for a highly complex supply chain. This might include, for example, a power plant outsourcing its catering to a supplier that has access to the organisation's IT network in order to manage catering for special events and meetings.[681] CNI firms may also outsource aspects such as CCTV and perimeter security; they source hardware and software from external providers; and potentially work with cloud providers to make their use of computational resources more cost-effective.[682] Most UK CNI organisations have multi-tiered supply chains

[676] Dourado, "Working Paper: Is There a Cyber Security Market Failure?."
[677] ibid.
[678] ibid.
[679] "Supply Chain." CPNI, accessed April 27, 2017. https://www.cpni.gov.uk/supply-chain.
[680] Interview with Cabinet Office employee.
[681] "Mitigating Security Risk in the National Infrastructure Supply Chain," CPNI.
[682] "Supply Chain," CPNI.

that are both upstream (i.e. between the organisation and the organisation's suppliers and even by extension those that supply its suppliers) and downstream (i.e. between the organisation and its market).[683] As the number of links in a supply chain increase, the task for a CNI organisation to manage the cyber security protocols of its suppliers becomes increasingly difficult. While an organisation might be confident of securing its own systems, products, services and data, it is much more difficult to protect these assets once they enter a wider supply chain.[684] This has led to real concerns – in a survey of senior CNI industry figures in the UK, fifty eight percent reported low levels of confidence in the cyber resilience of CNI supply chains, with half of those expressing no confidence at all.

The disharmony in the practices and actions between security actors leaves open security challenges that directly affect UK citizens. A cyber security market failure means that security actors are not appropriately prioritising the issue or investing in it appropriately. A responsibility deficit, where neither public or private actors are fully taking onus for addressing current cyber security challenges, with the interests of UK citizens not taken fully into account. Given the prevalence and entrenched nature of these partnerships what is arguably most worrying about this is the limited prospects for change in the future, given the stability of the current assemblage – suggesting that the current dynamics that have led to underinvestment may sustain in the long-term.

For the purposes of CNI, the security of individuals is paramount. In this regard, whilst the security of individuals is largely being provided by the UK CNI Assemblage, given the responsibility deficit outlined above, security provision is not at an optimal level. What is best for government actors and corporations is close to, but not completely correlated with, the

[683] "Mitigating Security Risk in the National Infrastructure Supply Chain,"
[684] "News Releases 2016," Atkins, October 20, 2016, http://www.atkinsglobal.com/en-gb/media-centre/news-releases/2016/oct/2016-10-20uk.

interests of individuals.[685] With private actors focused on keeping costs low and with government actors showing mixed messages about their desire to take on further responsibility, the vacuum in between these two represents a serious concern going forward.

At the same time, however, it should be realised that individuals drive some of the competing objectives faced by CNI security providers. Owners of CNI may underinvest in cyber security out of a desire to keep costs low, precisely because consumers desire low costs. For organisations including the NHS that are already stretched, it may not be rational to invest a significantly higher amount in cyber security at present, given the trade-offs this would involve (i.e. fewer doctors and nurses, longer wait time, etc.). Perspective is also required – ultimately, there have been few serious incidents of UK CNI being compromised by cyber attacks.

Yet, this does not mean that the market can efficiently provide the appropriate level of security. Most individuals have not considered the cyber security of CNI in depth and it is therefore unlikely to be a factor that is prominent in user demand, despite its importance. This enables CNI firms to get by without needing to substantially increase investment – particularly when they enjoy a level of dominance or even a monopoly in their industry. This does not mean that CNI should be nationalised – there are a number of good reasons why CNI should remain in private hands and government management of cyber attacks – as in the case of WannaCry shows that the UK Government actors also struggle to contain threats.

Yet CNI security could become a more prominent issue going forward as more threat actors develop offensive cyber capabilities and as the UK's digital dependence increases. The current situation may therefore prove unsustainable with CNI systems likely to be further targeted

[685] Carr, "Public–Private Partnerships in National Cyber-Security Strategies," 50.

going forward as has been observed in other regions including the US and Middle East.[686] If the cyber security of CNI does become a more prominent issue given shifts in threat actors, the dysfunctional aspects of the UK CNI Assemblage, and their impact on individuals, will only exacerbate and lead to further insecurity.

UK CNI Security Assemblage Chapter Conclusion

Similar to the previous case study, this chapter has shown that a vast array of security actors are involved in securing UK CNI. Although corporations are the primary actor in the assemblage, they work with various UK Government organisations, as well as other relevant actors including international actors, and academic actors. Moreover, the distinctions between corporations and the UK Government are blurring with a variety of shared practices leading to significant levels of hybridity.

This chapter has highlighted the unique insights that can be gained through an assemblage approach. The UK CNI Assemblage is dominated by what is often referred to as a public-private partnership, yet this case study has highlighted that distinctions between corporations and government actors are, at times, eroding due to the extent of shared practices that embed different actors into the same processes and institutions. This case study has therefore highlighted the way that traditional public-private and global-local distinctions are challenged by emerging cyber security structures and practices.

As well as focusing on power, an assemblage approach also considers the way that different security actors interact and compete for legitimacy. In this regard, an assemblage approach has provided a useful tool in studying a nascent security issue. Here, various actors (particularly in

[686] "TRISIS Malware Analysis of Safety System Targeted Malware" (Hanover, MD: Dragos, December 14, 2017); Chris Bing, "Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms," Cyberscoop, May 24, 2018, https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/.

government) have seen cyber security as an opportunity to expand their remit, creating competition between government actors that are all seeking to establish themselves as recognised cyber security authorities.

An assemblage approach also brings clear added value by highlighting the affect that often overlooked variables (including hybridity and harmony) have on security outcomes. The significant resources of corporations combined with mature and in-depth partnerships has created a high level of fusion through forms of public-private entrenchment. It would now be difficult for either corporations or the UK Government to disentangle itself from the hybrid structures that have emerged. In many respects, this is a good thing. Cooperation provides a means to overcome many of the ongoing challenges of keeping CNI secure. At the same time, however, it limits the UK Government's ability to significantly challenge, regulate and compel corporations. This would not necessarily improve the situation, yet the UK Government will nevertheless struggle to overcome or fix the concerns related to a corporation-led response to the cyber security of CNI (including possible market failures leading to inadequate investment).

With CNI security intrinsically linked to national security, it is reassuring that the vast majority of security actors within the UK CNI Assemblage work together and share a common view on security. The clashing securities observed in current encryption debates do not exist when it comes to CNI security. Yet, just because all the security actors want a secure CNI in theory, this does not mean that an optimal level of security has been achieved in practice. Despite a common objective to protect UK CNI, this chapter has shown that the dynamics and variables examined through an assemblage approach have led to numerous inefficiencies that could potentially inhibit CNI security in the long-term.

Chapter Five: The Estonian Digital Society Security Assemblage

Introduction

The Estonian Digital Society Assemblage represents a highly harmonious security structure. There is a significant level of hybridity within the assemblage – to the point that the majority of domestic security actors sit within an interunit cluster with distinctions between actors and sectors highly blurred. This has led to a highly stable assemblage dynamic with multiple actors sharing a common understanding of cyber security. With many of these dynamics existing in Estonia more broadly, it is clear that cyber security cannot be studied in a vacuum given that it is intrinsically linked to broader political, cultural, and historical factors.

In addressing the central research question of this thesis, the Estonian Digital Society Assemblage also provides new insights. The US case study highlighted the sub-optimal security outputs that can arise from negative assemblage dynamics while the UK Chapter showed a more mixed picture with both positive and negative assemblage dynamics leading to broadly positive, although at times inefficient, security outputs. This Estonia chapter, by contrast, is overwhelmingly positive. Crucially, this chapter shows how important the configuration and dynamic of an assemblage can be in creating a highly effective security structure. This is because the assemblage dynamics have enabled Estonia to overcome the natural limitations that exist for a small state possessing only limited resources and assert itself as a meaningful source of cyber security expertise in a global context.

The following case study explores the security of Estonia's Digital Society between May 2007 and May 2017. Given the close relationships and short communication links that exist within

Estonia, domestic security actors take on a prominent role. However, as a small state, Estonia is naturally inclusive and seeks to work closely with other stakeholders. Various international actors therefore also play an important role in securing Estonia's Digital Society.

Estonia's Digital Society: Overcoming the Legacy of the Soviet Union

Estonia's history explains why it is now one of the most technologically advanced countries in the world. Having regained independence from the Soviet Union in 1991,[687] the transition away from communism caused serious disruption. The small state's GDP was only around $2,000 per capita.[688] Many shops were completely empty with the Russian ruble no longer holding value.[689] Real wages fell by 45 percent, while overall price inflation was running at more than 1,000 percent.[690] Fuel prices had risen by more than 10,000 percent.[691] With minimal natural resources and a declining population, the Estonian government had to think creatively about the country's development[692] and subsequently became an aggressive early adopter of digital technology[693] that provided a relatively cheap means of enticing people to stay and do business in Estonia.[694] In some respects, the lack of investment in digital technology during the Soviet rule provided opportunities for Estonia: without legacy systems to consider, the state could leapfrog outdated technologies and instead turn straight to innovative technologies. The Estonian Government went from no land registry to an exclusively digital one for example.[695]

[687] "Estonia Celebrates the Day of Restoration of Independence," Estonian World, August 20, 2016, http://estonianworld.com/life/estonia-celebrates-the-day-of-restoration-of-independence/.
[688] Mart Laar, "The Estonian Economic Miracle," *Backgrounder* 2060 (August 2007): 1–12.
[689] ibid.
[690] ibid.
[691] ibid.
[692] Interview with Estonian Ministry of Defence employee by the author. Tallinn, Estonia. June 18, 2015; "Inside the World's Most Advanced Digital Society," Apolitical, July 7, 2016, https://apolitical.co/solution_article/estonia-digital-government-residency/.
[693] Cardash, Cilluffo and Ottis, "Estonia's Cyber Defence League: A Model for the United States?," 778.
[694] Interview with Estonian Government employee by the author. Tallinn, Estonia. February 11, 2016; "Inside the World's Most Advanced Digital Society."
[695] "How Did Estonia Become a Leader in Technology?"

Technology has played a crucial role in Estonia's growth ever since. The country declared Internet access to be a human right as early as 2000.[696] In 2017, Estonia had the third highest use of eGovernment services and had the highest proportion of prescriptions being made digitally within the EU.[697] Various technology companies (including Skype, Transferwise and Playtech), have all developed in Estonia.[698] Perhaps most significant, however, has been the emergence of a thriving 'digital society.'

Digital society is defined as the adoption of digital technology in a wide variety of functions and services used by the public. By 2017, Estonian government information systems consisted of 642 information systems in total, offering 4196 services, with 75,579 data objects, 12,133 personal data objects, which include 2384 delicate data objects.[699] Estonians have embraced a digital society culture, given the role technology has played in the state's rise and the country has been called 'the most advanced digital society in the world' by technology magazine Wired.[700] This is reflected through the public image Estonia seeks to project to the world: digital society (and related concepts including 'e-Estonia'), have become a crucial form of national branding[701] – initially as a means of presenting the country in a European context and in order to support Estonia's 'return to Europe'[702] while more recently the term has been used as a means of promoting the global competitiveness of Estonia and its openness to foreign

[696] This gave impetus to the deployment of Internet access in rural areas, and has driven innovative uses of digital technologies. See, Ivan Martinovic, Lucas Kello, and Ivo Sluganovic, "Blockchains for Governmental Services: Design Principles, Applications, and Case Studies," Working Paper Series, no. 7 (November 2017). pp. 8.
[697] "Digital Agenda Scoreboard Key Indicators."
[698] "Not Only Skype: Why a Small Baltic Country in Europe's North-East Is a Hotbed for Start-Ups," The Economist, July 11, 2013, https://www.economist.com/blogs/schumpeter/2013/07/estonias-technology-cluster.
[699] Jaan Priisalu and Rain Ottis, "Personal Control of Privacy and Data: Estonian Experience," *Health and Technology* 7, no. 4 (December 2017): 441–51. pp. 443.
[700] Ben Hammersley, "Concerned about Brexit? Why Not Become an e-Resident of Estonia," Wired UK, March 27, 2017, http://www.wired.co.uk/article/estonia-e-resident.
[701] Digital Society features as one of the three core messages developed by the Estonian government about the country that are intended to be the 'first things you can say about Estonia'. See, "Core Messages," Brand Estonia, accessed April 5, 2018, https://brand.estonia.ee/principles/core-messages/; Liina Areng, "Lilliputian States in Digital Affairs and Cyber Security," *The Tallinn Papers*, no. 4 (2014). pp. 4.
[702] Paul Jordan, "Nation Branding: A Tool for Nationalism?," *Journal of Baltic Studies* 45, no. 3 (2013): 283–303.

business and investment.[703] Yet, digital society is often discussed in a vague and loose way with the term used as an empty buzzword. To avoid such conceptual ambiguity, three essential features comprise the notion of digital society in the context of Estonia for the purposes of this case study are outlined below.

First, and most significantly, is the variety of digital services offered to citizens. Estonians have been able to file taxes online since 2000, vote in elections online since 2005 and blockchain has been in operational use in Estonia's registries since 2012.[704] Everything from prescriptions to court papers to the minutes of Estonia's Cabinet has been made paperless.[705] The government provided free public Wi-Fi in most populated areas as early as 2002. Today, Estonia is trying even more novel initiatives – an 'e-Residency' scheme launched in 2014 that allows non-Estonians to establish a virtual residency of sorts, enabling them to set up businesses in Estonia, access Estonian banking services, as well as digitally sign contracts and declare Estonian taxes online. German Chancellor Angela Merkel and Japanese prime minister Shinzō Abe are amongst its members[706] and the scheme has targeted British citizens looking to keep close ties to the European Union after Brexit.[707] It is this comprehensive adoption of digital services within a variety of contexts that sit at the heart of Estonia's digital society.

Second, the Estonian electronic ID (eID) infrastructure underpins and the majority of these Estonian digital services – a unique 16 digit personal identified number issued to every Estonian citizen at birth.[708] The system is based on a national population register that connects

[703] Piia Tammpuu and Anu Masso, "'Welcome to the Virtual State': Estonian e-Residency and the Digitalised State as a Commodity," *European Journal of Cultural Studies* (January 29, 2018).
[704] "We Have Built a Digital Society and So Can You," e-Estonia, accessed April 17, 2018, https://e-estonia.com.
[705] "Inside the World's Most Advanced Digital Society."
[706] Silver Tambur, "The Estonian President Invites Everyone to Become an E-Resident," Estonian World, December 1, 2016, http://estonianworld.com/business/estonian-president-invites-everyone-become-e-resident/.
[707] "How to Stay in – Manage an EU Company from the UK," e-Residency, accessed April 17, 2018, http://www.howtostayin.eu/.
[708] Helen Margetts and Andre Naumann, "Government as a Platform: What Can Estonia Show the World?," *Cyber Studies Research Paper* (February 28, 2017).

to a single unique national identifier for each Estonian citizen.[709] Possession of an Estonian electronic ID card is now mandatory for all permanent residents[710] although the Mobile-ID scheme allows Estonians to use their mobile phone as an alternative form of digital identification.[711] Each ID Card contains two digital certificates – one for authentication and one for signatures.[712] The authentication certificate is used to provide access to the variety of digital services outlined above: to access health care, to vote online in elections, or to take public transport.[713] The signature certificate is a digital equivalent of an ink signature. All Estonian authorities have been obliged to accept digitally signed documents since the Estonian parliament passed the Digital Signature Act in 2000.[714]

Third, the X-Road is a data exchange layer in Estonia, providing a link between national databases associated with Estonia's digital society.[715] A variety of data sources are required for Estonian digital services to operate effectively – ranging from healthcare to tax databases. This makes communication between databases vital. Estonia has developed an interoperability framework to ensure that the different government and private sector databases and systems are set up in a similar manner so that information can easily be transmitted and shared between different systems.[716] The Estonian digital infrastructure has also been setup to avoid duplication – information is only stored in one database[717] making the Estonian model highly decentralised and distributed.[718] Communication between different databases is therefore crucial – an

[709] ibid.
[710] Andrew Martin and Ivan Martinovic, "Security and Privacy Impacts of a Unique Personal Identifier," *Cyber Studies Programme Working Paper Series*, no. 4 (April 2016). pp.15.
[711] "Mobile-ID," e-Estonia, accessed April 18, 2018, https://e-estonia.com/solutions/e-identity/id-card/.
[712] Martin and Martinovic, "Security and Privacy Impacts of a Unique Personal Identifier,"15.
[713] "ID Card," e-Estonia, accessed April 18, 2018, https://e-estonia.com/solutions/e-identity/id-card/.
[714] Martin and Martinovic, "Security and Privacy Impacts of a Unique Personal Identifier," 14.
[715] "Data Exchange Layer X-Road," Estonian Information System Authority, accessed April 18, 2018, https://www.ria.ee/en/x-road.html.
[716] "Interoperability of the State Information System," (Tallinn, Estonia: Ministry of Economic Affairs and Communications, December 22, 2011); "Documents," Republic of Estonia Information System Authority, April 13, 2016, https://www.ria.ee/en/documents.html.
[717] "X-ROAD: A Secure Data Exchange Layer for Building e-Governments" (Tallinn, Estonia: Cybernetica, 2014), https://cyber.ee/uploads/2013/06/X-ROAD_technical_whitepaper_2014.pdf.
[718] Margetts and Naumann, "Government as a Platform: What Can Estonia Show the World?"

insurance service may require information about an individual's health records for example. The X-Road ensures that communication is secure. The three fundamental security conditions of the X-Road include that data is easily accessible by only those authorised to access and use it; that the integrity of data is maintained with no third parties able to make changes while data is in transit; and that data remains confidential and protected from unauthorised parties.[719]

This concept of digital society is increasingly important to security studies as well as IR more broadly. From an IR perspective, the concept of digital society leads to questions related to the changing character of states and state institutions. Estonia's digital society opens conceptual questions about what constitutes states and governments and the extent to which aspects of e-government should be regarded as core aspects of a nation-state (or not). From a security landscape, aspects of Estonia's digital society are stored and run in data centres outside of Estonia's borders (a point explored further in the Security Actors section) that leads to questions of whether aspects of a state's digital society – and by extension aspects of the Estonian government – ensure the continuity of state institutions even under conditions of military occupation (a very real concern in Estonia given the ease at which Russia could invade the state).[720] The security challenges of a digital society have also already been observed: various aspects of Estonian's online life were targeted by Russian hackers after the Estonian Government relocated a Russian war memorial from the centre of Tallinn to the city's outskirts. Between the 27th April to the 18th May 2007, Russian DDoS attacks took major Estonian papers' websites offline; government communications were unreachable; and cash machines and access to online banking went sporadically out of action.[721] Further, while Estonia is a

[719] infosysteemiamet, *X-Road Introduction (Long Version)*, 2016, https://www.youtube.com/watch?v=9PaHinkJlvA.
[720] Across multiple simulation games, a RAND study found that the longed it would take for Russian forces to reach the outskirts of Tallinn would be 60 hours. See, David Shlapak and Michael Johnson, "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics," (RAND Corporation, 2016).
[721] Florian Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates" (Oxford, UK: University of Oxford, 2018). pp. 148-151; Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, August 21, 2007, https://www.wired.com/2007/08/ff-

global leader in the development of a digital society, other states are heading in a similar direction: the UK Government's digital strategy has announced an intention to make public services 'digital by default;'[722] the 'Agenda Uruguay Digital 2020' aspires to make Uruguay an 'information society;'[723] while the 'National Digital Israel Initiative' seeks to 'adopt digital tools to lower the cost of living in Israel.'[724] Crucially, the vast majority of developed states are increasingly becoming digital societies in one form or another. The example of Estonia also shows how developing states can harness digital technology to their benefit. This process has already and will continue to increase levels of digital dependence – by extension, the cyber security of digital services is an increasingly important tenet of nationals security (a reality readily acknowledged in official Estonian policy documents).[725] Digital societies open up new challenges: for example, Estonia and other states that have introduced online voting are potentially exposed to adversaries that seek to interfere in their elections. Crucially, the uptake of a digital society is accompanied by increased digital dependence[726] – as the consequences of it failing increase, the topic becomes increasingly relevant for security studies. This chapter explores how assemblage dynamics affect the security of digital society infrastructure.

estonia/; McGuinness, "How a Cyber Attack Transformed Estonia."
[722] "Government Transformation Strategy," GOV UK, February 9, 2017, https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy.
[723] "Agenda Uruguay Digital 2020," Uruguay Digital, accessed April 18, 2018, https://www.agesic.gub.uy/innovaportal/file/125/3/agenda-uruguay-digital-2020---en.pdf.
[724] "The Digital Israel National Initiative: The National Digital Program of the Government of Israel," (Ministry for Social Equality, June 2017), https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf.
[725] "National Security Concept of Estonia" (Ministry of Defence, 2017), http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf; "Annual Cyber Security Assessment 2017," (Tallinn, Estonia: Estonian Information System Authority, 2017), https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF. pp. 5.
[726] Cardash Cilluffo and Ottis, "Estonia's Cyber Defence League: A Model for the United States?," 778.

Assemblage Configuration: a decisive government amidst volunteer and international actors

The security providers involved in the Estonia Digital Society Assemblage involves actors that are both specifically focused on aspects of Digital Society (such as digital services, electronic ID infrastructure and the X-Road) as well as actors that are concerned with the cyber security of national assets at a more general level. Indeed, the protection of national assets is increasingly inextricably linked with Estonia's Digital Society as an increasing number of digital services are introduced.

The Estonian approach to cyber security rests on a smooth cooperation between government actors, corporations, and civilian groups. Given both the prevalence of these three groups of actors (within the assemblage as a whole) and their levels of fusion, the use of clusters is not required with it instead possible to discuss the hybridity of the assemblage as a whole.

Government Actors

The Estonian Information System Authority (abbreviated as RIA after its Estonian title Riigi Infosüsteemi Amet) is the main government entity responsible for protecting Estonia's digital society. It is tasked with coordinating the development and administration of Estonia's information system.[727] The RIA is also responsible for drafting the Estonian Government's cyber security strategy[728] and developing relevant policy proposals.[729] One of RIA's primary

[727] "Information System Authority," Republic of Estonia Information System Authority, October 14, 2016, https://www.ria.ee/en/about-estonian-information-system-authority.html.
[728] It published Estonia's latest cyber security strategy for instance. See, "2014-2017 Cyber Security Strategy," (Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2014), https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.
[729] Anna-Maria Osula, "National Cyber Security Organisation: Estonia" (Tallinn, Estonia: NATO CCDCOE, 2015). pp. 7-8.

functions is through exercising supervision to ensure the continuous application of security measured used by systems related to Estonia's digital society infrastructure.[730] For example, the RIA is responsible for maintaining the X-Road and the state online portal, and coordinates the functioning of the public key infrastructure linked to eID.[731] In addition to developing legislation, policies and strategies related to Estonia's digital society, the RIA is also responsible for overseeing the compliance of such measures – including alignment with data protection laws and regulation for example.[732] RIA sits within the Ministry of Economic Affairs and Communication and has been the main cyber security body since 2011[733] – before which, RIA was formerly the Estonian Informatics Centre[734] and with core cyber security responsibilities for Estonia's digital society delegated to the Ministry of Defence. The RIA also has two sub-units, to which specific issues are delegated: the Department of Critical Information Infrastructure Protection (CIIP) and the Computer Emergency Response Team of Estonia (CERT-EE). In addition to an impressive strategic capability, RIA stands out from other government ministries with impressive technical expertise sitting within CERT-EE. RIA also provides penetration testing and other cyber security auditing services for various corporations, in order to test their security[735] – thereby demonstrating their technical understanding to a point that they can educate and scrutinise corporations involved both with CNI and digital services more specifically.

RIA has enjoyed significant political power in the Estonian Digital Society Assemblage since it took over as the main cyber security and digital society government entity in 2011.[736] It is

[730] Riigikogu, "Emergency Act" (2009), https://www.riigiteataja.ee/en/eli/525062014011/consolide.
[731] "Annual Cyber Security Assessment 2017," 2.
[732] Osula, "National Cyber Security Organisation: Estonia," 8.
[733] "Information System Authority."
[734] "The Estonian Informatics Centre Became the Estonian Information System's Authority," Republic of Estonia Information System Authority, June 16, 2011, https://www.ria.ee/en/the-estonian-informatics-centre-became-the-estonian-information-systems-authority.html.
[735] Interview with International Centre for Defence and Security researcher by the author. Skype. May 3, 2018.
[736] "Information System Authority."

responsible for drafting the Estonian Government's official cyber security strategy[737] and develops policy proposals related to Estonia's Digital Society infrastructure.[738] It also manages much of the relevant infrastructure, including X-Road, the underlying infrastructure that enables Estonia's Digital Society to function.[739] RIA takes on an administrative role for managing Estonia's Digital Society more broadly. This involves cataloguing various aspects of Estonia's Digital Society, including deciding which information systems and databases make up the official state's information system; what data is collected and processed (and in which information systems); which services (including X-Road) are provided and who is able to use them; the legal basis in which databases are operated and data is processed; and also establish which components of information systems should be interoperable, ensuring that databases run by different entities maintain consistent formatting.[740] Estonian Government entities have a track record of acting assertively in imposing its vision of Estonia's Digital Society: the early mandating of electronic tax filing in the 1990s led to an almost universal rate of electronic filing today and the X-Road has been made compulsory for government agencies.

The CIIP is tasked specifically with ensuring an appropriate level of cyber security in crisis situations. This involves the protection of vital services, defined as 'services necessary for organising the functioning of the society, healthcare, security and people's economical and social well-being'.[741] The CIIP seeks to ensure that such essential information and communication systems remain function in critical situations. Their purview clearly extends beyond digital society systems to include areas more directly associated with CNI (such as the

[737] It published Estonia's latest cyber security strategy for instance. See, "2014-2017 Cyber Security Strategy."
[738] Osula, "National Cyber Security Organisation: Estonia," 7-8.
[739] This includes hosting infrastructure, backup power for systems and digital archiving. See, "IT Infrastructure," Republic of Estonia Information System Authority, May 9, 2012, https://www.ria.ee/en/about-it-infrastructure.html.
[740] "Administration System for the State Information System RIHA," Republic of Estonia Information System Authority, February 29, 2012, https://www.ria.ee/en/administration-system-of-the-state-information-system.html.
[741] "Critical Information Infrastructure Protection CIIP," Republic of Estonia Information System Authority, June 10, 2017, https://www.ria.ee/en/ciip.html.

protection of energy, water and healthcare).[742] However, the all-encompassing nature of digital society means that it is inextricably entwined with many of these processes. The CIIP conducts risk analyses of critical information infrastructure and then initiatives and supervises the development and implementation of respective protective measures[743].

CERT-EE is another subunit of the RIA, responsible for the handling security incidents and analysing the spread of malware and incidents that have taken place on Estonian government computer networks – including those related to Estonia's digital society.[744] Its activities include handling security incidents (i.e. providing technical support and reporting on what has occurred); giving warning and notices about potential security gaps that, if discovered, may lead to systems being compromised; providing support for institutions and internet service providers involved in Estonian government computer networks and developing preventative measures (such as through organising awareness-raising events and media campaigns).[745] Compared to the rest of the RIA, CERT-EE operates on a more operational or technical level – responding to events as they occur rather than through developing more high-level and long-term strategy.

The Cyber Security Council was established in 2009 as an inter-department body to ensure that cyber security strategy and policy is implemented appropriately and the cooperation between government departments. It includes representatives from the Government Office, the Ministry of Economic Affairs and Communications, the Ministry of Defence, Ministry of the Interior, Ministry of Justice, Ministry of Finance, Ministry of Foreign Affairs, and the Ministry of

[742] The Estonian Emergency Act provides a list of 43 vital services that require protection. See, Riigikogu, "Emergency Act."
[743] "Critical Information Infrastructure Protection CIIP,"; Keir Giles and Kim Hartmann, "Cyber Defense: An International View" (Fort Belvoir, VA: Strategic Studies Institute and U.S. Army War College Press, September 1, 2015).
[744] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 192.
[745] "About CERT Estonia," Republic of Estonia Information System Authority, January 13, 2014, https://www.ria.ee/en/cert-estonia.html.

Science and Education.[746] It has been tasked to monitor the success of strategy related to cyber security and the protection of Estonian's digital society and submits annual progress reports outlining the realisation of objectives set out in strategy documents.[747] Despite the council being an inter-departmental body, this has not always ensured that its members are motivated to ensure the security of Estonia's digital society with various government departments showing insufficient interest and support in ensuring that cyber security policy was carried out (including at the cabinet level)[748] – most likely due to government departments prioritising other areas of policy development.[749]

With RIA taking the strategic lead on cyber security and the protection of Estonia's digital society, the Estonian executive branch plays a more hands-off role with the Prime Minister having minimal direct involvement on a day-to-day level.[750] The prime minister will however make a contribution at a high-level through policy proposals, managing government budgets, making speeches, etc. Here, it is clear the executive places a premium on the cyber security of Estonia's digital society with the topic often discussed in public appearances with Estonia's national branding including clear messages about both the sophistication of its digital society and its cyber security. The prime minister also becomes more deeply involved in the protection of Estonia's digitals society in crisis situations.[751]

The Ministry of Defence (MOD) previously had the strategic lead for cyber security and the protection of Estonia's digital society before this was handed over to RIA and the Ministry of

[746] Piret Pernik, "National Cyber Security Strategies The Estonian Approach" (International Centre for Defence Studies, June 22, 2017), https://www.cncs.gov.pt/content/files/estonian_cyber_security_strategy_-_piret_pernik.pdf.
[747] Osula, "National Cyber Security Organisation: Estonia," 7.
[748] Piret Pernik and Emmet Tuohy, "Greater Challenges" (International Centre for Defence Studies, August 2013). pp. 8.
[749] Interview with Estonian Government employee by the author.
[750] Estonia is a parliamentary republic where the Prime Minister enjoys executive power with the Estonian Presidency a ceremonial post.
[751] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 187–212.

Economic Affairs and Communication in 2011.[752] The MOD's cyber security purview has therefore reduced and become more focused over time, now centred on 'cyber defence in the area of national defence.'[753] Similar to the CIIP, the MOD's cyber security remit is more focused not the protection of CNI rather than digital society specifically – where digital society enters their purview is when the two concepts overlap (for example if critical healthcare systems were targeted that had following repercussions for healthcare digital services. The same also applies for the Estonian Internal Security Service (abbreviated as KAPO after its Estonian title Kaitsepolitseiamet), the primary intelligence arm of the Estonian government. KAPO is responsible for detecting and preventing cyber threats deriving from cyber intelligence, extremism, terrorism, and attempted sabotage.[754] KAPO's involvement in the protection of Estonia's digital society would only apply in limited instances – for example if a high-ranking Estonian official has been targeted by foreign intelligence services via digital society platforms.[755]

While RIA manages the central digital society infrastructure, each government ministry is responsible for the security of its own area. Each ministry therefore budgets cyber security independently. As digital technology is a significant part of Estonian culture, more government entities recognise that cyber security is important – especially given the increased levels of digital dependence caused from the high uptake of digital services. While security and defence institutions tend to prioritise cyber security, there are nonetheless 'weak spots' within the Estonian Government in areas that are not naturally defence oriented including healthcare and education where cyber security is one of many objectives.[756] RIA does however provide a

[752] "Information System Authority."
[753] "National Defence Strategy" (Tallinn, Estonia: Estonian Ministry of Defence, 2011), http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf. pp. 12.
[754] Osula, "National Cyber Security Organisation: Estonia," 12.
[755] "Estonian Internal Security Service Annual Review 2017" (Internal Security Service, 2017).
[756] Interview with International Centre for Defence and Security researcher.

supportive role for other ministries – including the issuing of guidelines, the provision of formats and penetration testing.[757] The centralised management of much of the digital society infrastructure also limits the extent of the incentive gap of other ministries.[758]

Civilian Groups

The security of Estonia's digital society goes beyond just a government responsibility. Indeed, as claimed by a then Estonian diplomat and now Undersecretary for Defence Policy at the MoD Kristjan Prikk, Estonian cyber security involves 'not just a whole of government approach, but a whole of nation approach.'[759] While other states have sought to overcome cyber threats by allocating vast budgets to the issue, Estonia has instead strived to create a state of digital-literate citizens alert to online threats.[760] Estonia operates a 'total defence model' (as is common with many small states),[761] whereby civilians are highly involved in the national defence due to a recognition that a professional armed force cannot provide an adequate level of security alone. This has traditionally applied to Estonia's conventional defence force with its reserve unit (the Voluntary Defence League) of about 15,000 vastly outnumbering the full time Estonian Regular Armed Force of 6,000.[762] Estonia's security presence can expand even more with its operational wartime structure capable of reaching around 60,000 personnel (with many Estonians who are not in the Voluntary Defence League still in a high readiness reserve).[763]

---

[757] ibid.
[758] ibid.
[759] Jackson, "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success," 6.
[760] ibid., Jamie Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 192.
[761] George J Stein, "Total Defense: A Comparative Overview of the Security Policies of Switzerland and Austria," *Defence Analysis* 6, no. 1 (1990): 17-33; Ron Matthews and Nellie Zhang Yan, "Small Country 'Total Defence': A Case Study of Singapore," *Defence Studies* 7, no. 3 (September 2007): 376–95; Charles E. Heller, "Economy of Force: A Total Army, the Israel Defense Force Model," (Strategic Studies Institute and U.S. Army War College, March 1, 1992).
[762] "Estonian Defence Forces," Kaitsevägi, accessed April 25, 2018, http://www.mil.ee/en/defence-forces.
[763] ibid.

In 2009, two cyber reserve units were created in Tartu and Tallinn as part of the corresponding regional units of Estonian Defence League. These two regional subunits were then reassigned into the Defence League Cyber Unit or Küberkaitse üksus (abbreviated as the CDL with the unit commonly referred to as the Cyber Defence League).[764] Cyber security was also included in The Estonian Defence League Act which passed in 2013 and outlines the key purpose, tasks, structure and legal bases for the activity of Estonia's reserve forces.[765] The CDL contains a broad range of skillsets, including not only those with a technical understanding but also legal or policy experts and educators.[766] Unlike the MoD's narrow cyber security purview (as discussed above), the CDL has a broader remit. Indeed, the protection of Estonia's digital society is listed as one of the CDL's main tasks – alongside engaging in public-private partnerships to protect internet infrastructure and sharing knowledge within Estonia.[767] It has also worked with CERT-EE, acting as a ready reserve during online elections and has organised table top exercises for Cabinet Ministers in 2012.[768]

With CDL members working on a voluntary basis, Estonia's Digital Society has access to a significant source of expertise that is able to make a meaningful contribution to its security. Estonia's cyber reserve is now more established and better organised as a formal part of Estonia's reserve force. The active role of the CDL also reaffirms core arguments of this thesis. From a theoretical and conceptual standpoint, the CDL's role in protecting Estonia's digital society shows that cyber security actors do not necessarily fall into neat public and private distinctions. From an empirical perspective, their presence also shows that the low barriers to

[764] Cardash Cilluffo and Ottis, "Estonia's Cyber Defence League: A Model for the United States?," 779.
[765] Riigi Teataja, "The Estonian Defence League Act" (2013), https://www.riigiteataja.ee/en/eli/525112013006/consolide.
[766] Kadri Kaska, Anna-Maria Osula, and LTC Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League," (Tallinn, Estonia: NATO CCDCOE, 2013). pp. 16.
[767] "The Main Tasks of the EDL CU," Kaitseliit, accessed April 26, 2018, http://www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu.
Cardash, Cilluffo and Ottis, "Estonia's Cyber Defence League: A Model for the United States?," 780.

entry within the cyber domain enable security actors other than large-scale actors (such as states, large defence contractors and international organisations).

Corporations

Since regaining independence in 1991, Estonia has developed a market economy approach that embraces a business culture and foreign investors. This belief in private industry is reflected in the makeup of Estonia's digital society with private sector outsourcing a common trend.[769] Digital society initiatives are therefore often developed by private businesses, with Estonian government entities only taking over the project once it is up and running.[770] Siim Sikkut, the Estonian Prime Minister's Digital Advisor and Chief Information Officer of the Estonian Government, has claimed that the Estonian 'government is a playground' as when companies have a "cool product idea", they can approach government to test it out in the public sector.[771] Private sector involvement in both the development and more critically to this thesis, the security of Estonia's Digital Society.

There is prevalent private sector involvement in the security of data in Estonia's digital society. This is clearly seen through the Keyless Signature Infrastructure (KSI) blockchain technology used to secure systems and data stored at rest associated with Estonian digital society and is used in a variety of digital services.[772] The distributed nature of a blockchain ledger means that changing or manipulating data is almost impossible. This means that the systems and date

[769] Meelis Kitsing, "Success Without Strategy: E-Government Development in Estonia," *Policy & Internet* 3, no. 1 (January 1, 2011): 1–21. pp. 16.
[770] Joshua Chambers, "Why Estonia Hasn't Built a Government Digital Service," GovInsider, May 10, 2016, https://govinsider.asia/digital-gov/why-estonia-hasnt-built-a-government-digital-service/.
[771] ibid.
[772] The list of Estonian State Agencies that are currently implementing and utilizing KSI blockchain technology include the: Healthcare Registry, Property Registry, Business Registry, Succession Registry, Digital Court System, Surveillance / Tracking Information System, State Gazette (official laws and Official State Announcements. See, Martinovic, Kello and Sluganovic, "Blockchains for Governmental Services: Design Principles, Applications, and Case Studies," 11.

centres underpinning Estonia's digital society are less reliant on trusting third parties and government insiders.[773] The KSI blockchain also improves the privacy of data: with only hashes of data stored in the KSI blockchain, the original document cannot easily be recreated by adversaries.[774] By 2016, the KSI blockchain reached an notable milestone as it secured all of Estonia's 1 million health records with its technology.[775] The role of Guardtime, an Estonian company established in 2007, has been critical in the development of the KSI blockchain. Guardtime developed the KSI blockchain and has grown into 'the world's largest blockchain company by revenue, headcount, and actual customer deployments.'[776] This role has been recognised by Estonian policymakers: according to Anna Piperal, the Managing Director of E-Estonia, 'With GuardTime KSI technology we don't have to trust anyone. We know that our data was safe. Guardtime is empowering Estonian Government mission critical data security and integrity.[777]

Crucially, corporations feature prominently in all three of the core aspects of Estonia's Digital Society outlined in the introduction. A variety of Estonian firms were instrumental in developing the X-Road[778] including: Aktors,[779] Cybernetica,[780] and Nortal[781] that developed the underlying infrastructure while Andmevara developed the Population Register,[782] Datel developed the e-land register,[783] and Roksnet developed the international X-Road linked with

[773] "eGovernment," Guardtime, accessed April 27, 2018, https://guardtime.com/solutions/egovernment; "Security and Safety," e-Estonia, accessed April 5, 2018, https://e-estonia.com/solutions/security-and-safety/.
[774] Martinovic, Kello and Sluganovic, "Blockchains for Governmental Services: Design Principles, Applications, and Case Studies," 12.
[775] Omri Barzilay, "3 Ways Blockchain Is Revolutionizing Cybersecurity," Forbes, August 21, 2017, https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/.
[776] ibid.
[777] Rasmus Merivoo, "Anna Piperal - Ambassador of E-Estonia," accessed April 27, 2018, https://www.youtube.com/watch?time_continue=75&v=bvEQrn9oVaU.
[778] "X-Road," e-Estonia, accessed April 30, 2018, https://e-estonia.com/solutions/interoperability-services/x-road/.
[779] "Portfolio," Aktors, accessed April 30, 2018, http://www.aktors.ee/en/portfolio.html#xroad.
[780] "X-Road," Cybernetica, accessed April 30, 2018, https://cyber.ee/en/e-government/x-road/; "X-ROAD: A Secure Data Exchange Layer for Building e-Governments."
[781] "X-Road," e-Estonia.
[782] "Digitisation," Andmevara, accessed April 30, 2018, https://www.andmevara.ee/en/web/eng/digitisation.
[783] "E-Cadastre," Datel, accessed April 30, 2018, http://www.datel.eu/en/solutions/e-government-

Finland.[784] From a digital services perspective, NETgroup and Aktors developed the Estonian e-Court[785] while Nortal developed data governance and data protection mechanisms.[786] In addition to the KSI Blockchain, Guardtime also developed e-Law and e-police services.[787] Likewise, corporations have also been active in the development of online identity schemes.[788] Both Politsei- ja Piirivalveamet[789] and Raul Walter[790] have developed the Estonian digital systems while Signwise developed the digital signature system.[791] Teila.[792] Nortal,[793] and SK ID Solutions[794] have also been behind mobile-ID initiatives. Estonian Government entities develop a clear idea of the solutions they want before government contracts are awarded – meaning that security is considered throughout the process as these financially-motivated firms develop aspects of Estonia's Digital Society.[795] Where an incentive gap is more acute is with small and medium enterprises that while not a direct part of Estonia's Digital Society, may, for example be involved in systems linked to Estonia's digital services in areas such as healthcare.[796]

US-based technology firm Microsoft is also a part of the Estonian Digital Society Assemblage, involved in the data embassy project discussed in the Government Actors section above. In addition to both Estonian government clouds located in its borders, and the sovereign data

solutions/item/232.
[784] "Government," Roksnet, accessed April 30, 2018, https://www.roksnet.com/government.
[785] "Aktors," e-Estonia, accessed April 30, 2018, https://e-estoniax.com/.
[786] "Data Protection," Nortal, accessed April 30, 2018, https://nortal.com/business/data-protection/; "Security and Safety," e-Estonia, accessed April 5, 2018, https://e-estonia.com/solutions/security-and-safety/.
[787] ibid.
[788] "e-Identity," e-Estonia, accessed April 30, 2018, https://e-estonia.com/solutions/e-identity/id-card/.
[789] "Identity Documents," Politsei- ja Piirivalveamet, accessed April 30, 2018, https://www2.politsei.ee/en/teenused/isikut-toendavad-dokumendid/.
[790] Antenn, "Digital Identity Management," RaulWalter, accessed April 30, 2018, https://www.raulwalter.com/government/digital-identity-management/.
[791] "Overview," Signwise, accessed April 30, 2018, https://signwiseservices.com/#overview.
[792] "Mobile ID," Telia, accessed April 30, 2018, https://www.telia.ee/en/era/mobiil/lisateenused/mobiil-id.
[793] "Mobile ID Is an Electronic Identity and Digital Signature Solution," Nortal, accessed April 30, 2018, https://nortal.com/government/electronic-identity/mobile-id/.
[794] "Mobile-ID," SK ID Solutions, accessed April 30, 2018, https://sk.ee/en/services/digital-identity/mobile-id/mobile-id.
[795] Interview with International Centre for Defence and Security researcher.
[796] ibid.

centre located in Luxembourg, the Microsoft Azure cloud computing platform also plays an active role in ensuring the security and continuity of Estonian digital services. Microsoft has also helped to backup and secure non-sensitive databases, such as the Estonian land registry.[797]

Corporation have significant material capabilities within the Estonian Digital Society Assemblage. This is largely due to the technical skills possessed, meaning that corporations are active at an operational level in protecting the Estonian Digital Society Assemblage. This includes a prominent role in of a range of services protecting the digital society, including threat intelligence, research, and penetration testing.[798] A long-standing adviser to RIA claimed that Clarified is one corporation with a significant material capability that is highly active protecting Estonia's Digital Society.[799] The firm itself claims that its home market is the 'IT Wonderland of Estonia' and its main offering is manual web application penetration testing, playing an integral part in ensuring the security of Estonian digital services applications.[800] Corporations also bring technical expertise to government cloud solutions (as discussed further in the second exemplar) .

International Organisations, Networks, and Partners

A core argument of this thesis is that various actors are seeking to establish relevancy as cyber security providers. This is one of the driving forces behind the emergence of complex structures (or assemblages) that provide security in a given context. This is clearly seen in regard to international organisations and networks that are expanding their remit to accommodate the issue of cyber security – a trend previously observed in the UK CNI Assemblage. As the

[797] "Transforming Digital Continuity" (Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, May 2016).
[798] Interview with Andres Kutt (former Chief advisor to RIA). Skype. May 16, 2018.
[799] ibid.
[800] "# We Break Security to Bring Clarity," Clarified Security. Accessed August 5, 2018, https://www.clarifiedsecurity.com/.

Assemblage Dynamics section of this chapter will show, Estonia is highly receptive to international involvement in cyber security and the security of its digital society, thereby providing clear opportunities for international actors to develop.[801]

The EU is seeking to establish itself as a relevant and meaningful cyber security actor in the context of the European project. This applies not only to CNI (as discussed in Chapter Four) but also in the development and security of a digital society. The European Commission has made the development of the 'digital single market' a priority with an emphasis on building eGovernment solutions – an initiative that relates directly to Estonia's Digital Society.[802] The EU eGovernment action plan has declared an ambition to digitise various functions and processes including identification, certificates, invoices, and procurement systems (amongst other areas).[803] It also intends for various digital services and instances of eGovernment to become interoperable across the EU – thereby resulting in a shared understanding of security.[804] The Ministerial Declaration on eGovernment (also known as the Tallinn Declaration given that it was signed during Estonia's EU presidency) frames the security challenges of eGovernment as a European challenge.[805] The EU also provides security in other ways in the context of Estonia's Digital Society. EU Structural Funds have provided RIA with additional money to invest in cyber security[806] with the scheme Raising Public Awareness about the Information Society receiving five million euros to raise awareness of the security challenges related to Estonia's Digital Society and how service infrastructure can be improved.[807] The EU also runs

[801] "2014-2017 Cyber Security Strategy," 12-13; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 194-195.
[802] "Digital Agenda Scoreboard Key Indicators."
[803] "EU eGovernment Action Plan 2016-2020: Accelerating the Digital Transformation of Government" (European Commissioner, April 19, 2016). pp. 4.
[804] "New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations" (European Commissioner, 2017). pp. 4.
[805] "Tallinn Declaration on EGovernment at the Ministerial Meeting During Estonian Presidency of the Council of the EU" (EU2017, October 2017). pp. 3-5.
[806] Interview with International Centre for Defence and Security researcher.
[807] "Raising Public Awareness about the Information Society," Republic of Estonia Information System Authority, December 28, 2015, https://www.ria.ee/en/programme.html.

its own CERT (CERT-EU) and coordinates cooperation amongst CERTs in the block – Estonia is also a member of FIRST, the international CERT network.[808]

The Estonian Government has been eager to develop cooperation in either small groups or on a bilateral basis. It has built on pre-existing ties with its allies in the Nordics and Baltic, leading to bilateral and regional cooperation on cyber security that involves elements of Estonia's digital society.[809] It has also forged alliances further afield with states including the US[810] and Japan.[811] Foreign government entities have forged close partnerships related directly to the security of Estonia's digital society.[812]

Estonia also invests much attention into cooperation with the Nordic-Baltic countries, both as a group and bilaterally. That encompasses cyber defence technical information sharing and assistance, pooling of resources, and inter-agency cooperation. All states in the Nordic-Baltic region are small and are therefore compelled to work more closely together.[813] The Nordic Institute for Interoperability Solutions is a non-profit foundation cofounded by the Estonian Ministry of Economic Affairs and Communications and the Finnish Ministry of Finance to develop and facilitate an X-Road to link the two countries' digital services and data.[814] This has led to active collaboration between the two governments over the security of X-Road

[808] "FIRST Teams," FIRST, accessed May 4, 2018, https://www.first.org/members/teams/.
[809] Interview with International Centre for Defence and Security researcher; "Estonia Ready to Share Cyber Security Expertise with Iceland," Republic of Estonia Ministry of Foreign Affairs, June 20, 2017, http://vm.ee/en/news/estonia-ready-share-cyber-security-expertise-iceland.
[810] John Kerry and Urmas Paet, "Remarks at a Cyber Partnership Agreement Signing With Estonian Foreign Minister Urmas Paet" (Brussels, Belgium, December 3, 2013); Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 194-195.
[811] Sten Hankewitz, "Estonia and Japan to Sign a Cyber Security Cooperation Treaty," Estonian World, December 18, 2017, http://estonianworld.com/security/estonia-japan-sign-cyber-security-cooperation-treaty/.
[812] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 194-195.
[813] Areng, "Lilliputian States in Digital Affairs and Cyber Security," pp.9.
[814] "Trust Federation of Estonian X-Tee and Finnish Palvelyväylä: General Agreement Between Estonian Information System Authority and Finnish Population Register Centre," (Estonian Information System Authority and Finnish Population Register Centre, September 29, 2016), https://esuomi.fi/wp-content/uploads/2016/09/RIA_VRK_Trust_federation_Agreement_.pdf; "Estonia and Finland to Develop the X-Road Together," ShowTime, October 6, 2017, https://www.ria.ee/en/estonia-and-finland-to-develop-the-x-road-together.html.

infrastructure.[815] This included Finland's Population Register Centre introducing technical changes into X-Road in 2016 to include a monitoring option added to the infrastructure, enabling platforms administrator to better examine the functionality of the services.[816] Estonia's RIA and the Finnish Population Register Centre also jointly audited code associated with X-Road.[817]

Other international actors and networks play an active role in Estonia's cyber security more broadly – and thus by extension in the security of Estonia's Digital Society. Since the 2007 attacks, the Estonian Government has been a proponent of NATO extending NATO's remit into the cyber domain.[818] This role has grown over time – the international organisation initiated the development of a unified strategy against cyber attacks in 2017 and adopted the new strategic concept that recognises cyber attacks as a threat to the alliance and opts for the enhancement of alliance's and nations' capabilities to face the threat in 2010.[819] So far, NATO's role is largely restricted to defending its own networks, yet it contributes to the cyber security of Estonia, and its digital society through its deterrent effect. Estonian government actors have been an active proponent of NATO's Article 5 extending to the cyber domain and as discussed in Chapter Three, NATO officials have since confirmed that Article 5 applies to the cyber domain, thereby enabling the principle of collective defence. The NATO CCDCOE is located in Tallinn and hosts the annual Locked Shield cyber crisis simulation exercise. The CCDCOE also provides a vehicle for expanding NATO's role in a cyber security context through

[815] ibid.
[816] "Annual Cyber Security Assessment 2017," 48.
[817] ibid., 48.
[818] Czosseck, Ottis, and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security"; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 194-195.
[819] Czosseck, Ottis, and Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security."

publications and events that raise awareness of cyber security and the ways in which NATO can play a role in providing cyber security.

The majority of international organisations and networks provide assistance at a strategic or high-level. There are, however, more focused technical capabilities offered from abroad. This includes the FIRST network of CERTs where the security of Estonia's Digital Society is supplemented by threat intelligence and technical insights provided by the broader global community of CERTs – for example, a threat targeting Estonia's Digital Society infrastructure might have previously targeted other systems outside of Estonia and other CERTs can help CERT-EE to understand and mitigate the threat at hand. Further, many of the memorandums of understanding between Estonia and other states, as well as other forms of bilateral cooperation, can lead to meaningful exchanges.[820] Cooperation between Estonia and the US involved information sharing between key institutions including the US National Cyber Security and Communications Center and the US Computer Emergency Readiness Team (US-CERT with RIA and CERT-EE in particular. Cooperation has also involved an exchange of government employees, enabling Estonians to learn and understand the technical and operational insights from some of the most capable cyber security states.

In addition to the main international security providers in the Estonia Digital Society Assemblage outlined above, there are other international organisations and networks that are more tangentially relevant. Estonia is part of the 'Digital 7'[821] – a network of leading digital governments that also includes Canada, Israel, New Zealand, South Korea, the UK, and Uruguay. This has also led to bilateral cooperation with specific members: the UK Government

[820] Interview with Andres Kutt.
[821] Formerly known as the Digital 5 before Canada and Uruguay joined in February 2018. See Matteo Natalucci, "Canada and Uruguay Join Digital 5 Government Group," Government Computing Network, February 22, 2018, http://central-government.governmentcomputing.com/news/canada-and-uruguay-join-digital-5-government-group-6063639.

has embedded a team in its Tallinn embassy known as TechLink to develop digital partnerships between the UK and Estonia.[822] While both the Digital 7 and initiatives such as TechLink discuss cooperate on issues related to Estonia's digital society, cooperation on the cyber security is limited only to high-levels discussions. Estonia is also involved in the UN GGE (as discussed in Chapter Three) and is part of an informal working group for developing confidence building measures in cyberspace at the Organization for Security and Co-operation in Europe.[823]

Assemblage Dynamics: hybrid and harmonious relationships within a small state

The previous section outlined that the vast majority of actors share a common interest in protecting Estonia's Digital Society. This has created a highly harmonious, hybrid and stable assemblage.

Internal Processes

The Estonian Digital Society Assemblage is a highly harmonious structure and much of this is due to the convergence of interests between actors. There are no significant examples of clashing securities, the incentive structures of actors are well aligned and the broader Estonian cyber security community comes together to confront challenges related to the security of its digital society infrastructure. Even for Estonian Government actors that are not primarily cyber security actors, including the Ministry of Education and Research and the Ministry of Social Affairs, they still actively use and interact with digital services and systems on a day-to-day

[822] "About Us," TechLink, accessed May 3, 2018, http://ukesttechlink.com/about-us/.
[823] "2014-2017 Cyber Security Strategy," 4.

basis, meaning cyber security is still taken seriously.[824] The high levels of harmony within the Estonia Digital Society is also influenced by variables not primarily examined in this case study or thesis: its size. Estonia benefits as a small state from a well-connected 'everyone knows everyone' society.[825] These national characteristics that encourage positive relationships between different actors and individuals outline above are also reflected through converting incentive structures between different security actors.

There is also a broad distribution of power across the assemblage. While corporations possess a significant portion of the technical capability, Estonian Government actors nonetheless have a significant degree of political power (which has been largely respected by other actors within the assemblage). This is largely reflected through legislation related to the provision of 'vital services' by both state and local government authorities. For instance, Section 40 of the 2009 Emergency Act obliges providers to ensure a 'constant application of various security measures in regards to the information systems used for the provision of the vital service and the related information assets.'[826] New legislation introduced in May 2018 creates more formal requirements for corporations, making it compulsory to them to partake and submit cyber security auditing procedures and in following governmental standards.[827]

There are also positive levels of harmony within the Estonian Government. Across the whole of the Estonian Government there is a broad recognition that the security of Estonia's Digital Society is important. This leads to positive relationship between Estonian Government entities for three reasons. First, there are not significant incentive gaps for non-security government entities. Second, given the above, To further enhance coordination and goodwill between

[824] Interview with researcher at Tallinn University of Technology by the author. Skype. May 18, 2018.
[825] Interview with Estonian Ministry of Defence employee; Interview with International Centre for Defence and Security researcher.
[826] Riigikogu, "Emergency Act," Chapter 4, Section 40.
[827] "Küberturvalisuse seadus 597 SE" (2018), https://www.riigikogu.ee/tegevus/eelnoud/eelnou/; Interview with Ministry of Economic Affairs and Communications Legal Advisor by the author. Skype. May 17, 2018.

government entities on the issue of cyber security, the Cyber Security Council was established in 2009 as an inter-agency advisory, supervisory and coordination body that has supported efforts to develop cooperation between government entities and to oversee the implantation of official cyber security strategy objectives.[828] RIA forms the central cyber security provider, and takes on the central administrative role for Estonia's Digital Society more broadly, responsible for the transparency of the administration of the state's information system. While RIA's role is largely respected, it also works well with the other government ministries and public bodies that are assigned by the Emergency Act as responsible for managing the continuous operation of vital services with cyber security an important component of this responsibility[829] (many of which are highly relevant to the protection of Estonia's Digital Society. Various government entities therefore manage different databases related to their area.[830] Where such decentralisation does occur, however, it has occurred within a highly ordered structure. The extent to which various government actors develop independently and become separate entities is also limited through the processes in which responsibility and authorise can become quickly centralised to the Executive. While the Prime Minister's office typically plays a hands-off role in the Estonia Digital Society Assemblage, this changes in crisis situations for instance. The 2009 Emergency Act requires providers of vital services to immediately notify the relevant national government department about attacks. Governmental powers can be further escalated through the 1996 State of Emergency Act if a threat emerges that threatens the constitutional order of Estonia (which could include serious cyber attacks).[831] Given that Estonia's Digital Society is now linked to fundamental understandings of national security in Estonia, this means

[828] "Cyber Security," Republic of Estonia Ministry of Economic Affairs and Communications, October 5, 2017, https://www.mkm.ee/en/objectives-activities/information-society/cyber-security; Pernik and Tuohy, "Cyber Space in Estonia: Greater Security, Greater Challenges," 8.
[829] "Section 34, Emergency Act" (2009), https://www.riigiteataja.ee/en/eli/525062014011/consolide; Dimitra Liveri and Anna Sarri, "Critical Information Infrastructures Protection Approaches in EU," 2015, 19.
[830] Interview with International Centre for Defence and Security researcher.
[831] "State of Emergency Act" (1996), https://www.riigiteataja.ee/en/eli/530122013002/consolide; Osula, "National Cyber Security Organisation: Estonia," 10-11; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 191-192.

that attacks on digital services and critical databases connected to Estonia's Digital Society could plausibly trigger the State of Emergency Act.[832] The act significantly centralises political power by concentrating rights, duties, and liabilities in the Prime Minister.[833] Political power is thus context-dependent in the Estonia Digital Society Assemblage from a governmental perspective: political power is typically vested in the RIA and with other ministries responsible for managing cyber security issues within their remit while the Prime Minister's Office plays a significantly expanded role in crisis situations.[834]

There is also a healthy relationship between Estonian Government actors and corporations. Corporations make an important and positive contribution to the security of Estonia's Digital Society – indeed, official government strategy documents and statements acknowledge the important role that corporations should play in the security of Estonia's Digital Society.[835] This is explained by the incentive structures of corporations. After all, they all regularly rely on various aspects of digital society infrastructure and corporations use and depend on the same digital infrastructure – whether that be using digital signatures for contracts, requesting data from government databases, developing integrated e-services or in also using X-Road.

As was observed in the UK case study, the salaries demanded by cyber security talent has provided one of the main reasons why material power lies with corporations – a situation also observed in Estonia and one of the main reasons why RIA outsources a significant degree of developing and securing Estonia's Digital Society. Sikkut claimed that 'you cannot really hire

[832] Osula, "National Cyber Security Organisation: Estonia," 10-11.
[833] "State of Emergency Act" (1996), https://www.riigiteataja.ee/en/eli/530122013002/consolide.
[834] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 191-192.
[835] "2014-2017 Cyber Security Strategy," 5; "Annual Cyber Security Assessment 2017," 4.

programmers on our payroll' given that Estonian Government entities are competing with companies such as Skype, which still has a significant presence in Estonia.[836]

The security of Estonia's Digital Society is an important objective for many Estonian-based corporations. Part of cyber security firm Nortal's vision is to transform Estonia into a digital leader and build a seamless society for example.[837] Further, the strong cyber security community and the involvement of many corporation employees in the CDL (and also doing stints working for government entities) means that there is a degree of trust within the cyber security community.

Further, corporations have primarily been used to initially develop aspects of Estonia's Digital Society. It is here where government actors face limitations in being able to do this themselves (given resource and salary constraints). However, once systems have been developed, they are then typically taken over by RIA or other relevant government actors. In this regard, corporations are primarily responsible for the development rather than the maintenance of Estonia's Digital Society infrastructure.

Of course, the Estonian Digital Society Assemblage does have instances of tension and divergent incentive structures. Despite the broadly understanding tone of corporations in relation the new cyber security regulation that bolsters the political power of RIA, certain corporation (particularly those related to the telecommunication industry) have resisted these calls for change.[838]

The Estonia Digital Society Assemblage also stands out as a security structure with remarkable levels of fusion between actors. A crucial component of the positive assemblage relationships

[836] Chambers, "Why Estonia Hasn't Built a Government Digital Service."
[837] "Building a Seamless Society," Nortal, accessed April 5, 2018, https://nortal.com/.
[838] Interview with Ministry of Economic Affairs and Communications Legal Advisor.

within Estonia is underpinned by a 'whole of nation' approach to cyber security. Given the role of digital technology in overcoming the legacy of the Soviet Union, there is now a close linking between notions of the state and national identity with Estonian Digital Society and its e-government services.[839] This is significant given the culture that exists within the whole of nation approach to national defence and security. As previously outlined in the Security Actors section, Estonia's total defence model means there is a culture of corporations and civilian involvement in national defence – which, given the close linking of national security and digital society security means that Estonia's total defence model has been extended into the cyber security of Estonia's Digital Society. Although much of the technical and operational cyber security capability lies outside of Estonian Government entities, a holistic approach to cyber security means that digital society infrastructure, remains well protected – whether by governmental or non-governmental entities. The role of the CDL provides the clearest example of this approach, yet corporations also play an active voluntary role.[840]

There is a very close and active cyber security community in Estonia, comprising those from government, corporations and academia. Rather than certain organisations, it is this collective cyber security community that sits at the heart of the protection of Estonia's Digital Society. While different actors and organisations do work together to provide security, the positive relationships and willing to cooperate amongst individuals is more significant. As one interviewee claimed in relation to the Estonian cyber security community, 'organisations don't cooperate, people do.'[841] The distinctions between organisations and actors therefore becomes blurry when examining security provision in the Estonian Digital Society Assemblage.

[839] Interview with Andres Kutt.
[840] Interview with Estonian Government employee by the author.
[841] Interview with Andres Kutt.

With many of the employees working for corporations involved in developing and protecting the Estonian Digital Society Assemblage also members of the CDL, there is naturally overlap in their capabilities with the distinctions between the two actor types often difficult to establish. While the CDL and corporations therefore draw on a very similar stock of people (and with the distinction between the two somewhat artificial), the CDL material capability is limited by organisational restraints: as a voluntary organisation that relies on members to contribute in their spare time,[842] it is better suited to ad hoc responses in crisis situations (as it was designed to do) rather than for more sustained, full-time projects that require greater resources.

The Estonian cyber security community, however, goes beyond just facilitating cooperation between actor types and actually creates an environment where an individual's contribution to the protection of Estonia's Digital Society is directly tied to their career capital. The Estonian cyber security community meets once a quarter for an initiation-only two to three days that combines technical talks and workshops with social events.[843] In addition to building goodwill within the community and between corporations and government entities, these events are crucial for career development. Those unwilling to contribute to the community and the security of Estonia's Digital Society will lose their invitation – and may also lose invitations to invite-only training sessions and access to a security clearance.[844] Career capital is therefore directly linked to participating in the broader community, thereby creating a self-policing dynamic where Estonian cyber security experts have very clear reasons to develop positive harmonious relationships with one another.[845]

[842] "The Main Tasks of the EDL CU,"; "Estonian Defence League's Cyber Unit," Kaitseliit, April 24, 2018, http://www.kaitseliit.ee/en/cyber-unit; Kaska, Osula, and Stinissen, "The Cyber Defence Unit of the Estonian Defence League," 45; Cardash Cilluffo and Ottis, "Estonia's Cyber Defence League: A Model for the United States?,".
[843] Interview with Andres Kutt.
[844] ibid.
[845] ibid.

Another important feature of the Estonian Digital Society Assemblage dynamics is the way it is highly conducive to international involvement. Robert L Rothstein has previously observed that a small state typically recognises 'that it cannot obtain security primarily by the use of its own capabilities, and that it must rely fundamentally on the aid of other states, institutions, processes, or developments to do so.'[846] This is reflected practically in Estonia's commitment to international organisations. Emphasis is placed on developing cyber security cooperation at a bilateral, regional and multilateral level in Official Estonian Government Cyber Security Strategy[847]. As reported in 2014, 'Estonia is the only country in Europe that meets the rules of every club to which it belongs. It meets the euro zone's targets on debt, inflation and government deficit, as well as NATO's standard: 2 percent of GDP on defence.'[848] It hosts the NATO CCDCOE, has been a chief advocate of extending NATO's cyber security remit,[849] develop close ties with several Nordic states,[850] and used its Estonian Presidency term to raise awareness of cyber security cooperation.[851] Estonians are therefore largely supportive of international organisations and networks taking on an expanded cyber security role.

The EU has the most significant political power out of the relevant international organisations and networks in the Estonia Digital Society Assemblage. The EU has substantially increased its remit in relation to technology and issues that relate to Estonia's Digital Society in the last ten years.[852] There has been a notable trend of relevant issues being changed from directives to regulation – a phenomena already observed in relation to Electronic Identification and Trust

[846] Robert L Rothstein, *Alliances and Small Powers* (New York: Columbia University Press, 1968). pp. 29.
[847] "2014-2017 Cyber Security Strategy," 12 -13.
[848] Edward Lucas, "Against Putin, It's Time to Channel JFK," POLITICO Magazine, August 22, 2014, http://www.politico.com/magazine/story/2014/08/only-obama-can-stop-putin-now-110264.html.
[849] Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 195.
[850] Areng, "Lilliputian States in Digital Affairs and Cyber Security," 9; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 195.
[851] This included various initiatives, including the security of the 'digital single market', developing a stronger EU regulatory framework, and educational projects. See, "Cybersecurity and the Estonian Presidency," EU2017.EE, August 3, 2017, https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency.
[852] Interview with Laura Kask.

Service Regulation as well as General Data Protection Regulation that both increase the EU's political powers. It has also been predicted that the Network and Information Security Directive[853] will follow this trend in eventually becoming regulation.[854]

Estonian Government actors have realised that as the EU expands its digital remit, it will inevitably lead to compromises that do not always suit Estonian interests.[855] Yet, none of these disputes have had a significant impact on the nature of security provision and do not undermine the broadly highly positive and harmonious relationships between security actors. Further, Estonian Government actors also see opportunities in an EU context. Estonia has put in significant effort to convert other EU states to its way of thinking – both on developing digital society processes and on cyber security cooperation (not that other states always share such a vision).[856] The sophistication of Estonian digital services means that it often plays an active and often outsized (relative to its size) role in EU technology policy developments and enabled Estonia Government actors to export its vision internationally.[857] The notion of the free movement of data was a key aspect of Estonia's EU Presidency for example. Estonia has therefore been at the forefront of seeking to increase the digital remit of the EU, given the Estonian Government's opportunity to make a significant contribution and due to the business opportunities it could unlock for Estonian corporations that have experience and expertise in developing digitals society infrastructure.[858] Estonia's accommodation of international networks and organisation converges with the incentive structures of these actors themselves – many of whom regard cyber security as an opportunity to expand their remit.

[853] "The Directive on Security of Network and Information Systems (NIS Directive)," European Commission, July 5, 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[854] Interview with Laura Kask.
[855] Interview with Laura Kask.
[856] "Estonia Is Trying to Convert the EU to Its Digital Creed," The Economist, July 6, 2017, https://www.economist.com/news/europe/21724831-country-e-residency-wonders-why-others-are-more-sceptical-estonia-trying-convert.
[857] Interview with Ministry of Economic Affairs and Communications Legal Advisor.
[858] Ibid.

With the NATO CCDCOE based in Tallinn, it is also an important player in the Estonian Digital Society Assemblage. While predominantly a research centre, its political impact in Estonia is often more clearly seen through its second order-effects. As previously discussed in Chapter Three, the centre hosts an annual Locked Shields cyber crisis exercise that brings governmental cyber security teams across NATO states to Estonia. Further, the distinctions between what is an international organisation and what is s domestic Estonian actor have become blurred with the NATO CCDCOE in many ways achieving Estonian interests. The centre is predominantly staffed by Estonians and the simulation exercises, conferences and research initiatives that it hosts have previously brokered connections in and brought money into Estonia in a cyber security context.[859]

Evolution

The Estonian Digital Society Assemblage has evolved in a highly stable manner without significant changes occurring. The broadly positive harmony and converging interests between different security actors therefore appears set to continue.

There are nonetheless two important shifts that have occurred over time: the further growth of the Estonian Government's political power and the emergence (and increased accommodation) of international actors and networks. Estonian Government actors have gradually grown their purview and authority on issues related to the cyber security of digital society. Part of this simply relates to Estonian Government actors' role increasing as new initiatives are launched – such as the Data Embassy project, or the introduction of the e-residency programme. The

[859] Interview with Andres Kutt.

role of Estonian Government actors has naturally therefore expanded in line with the growth of digital society.

Yet, Estonian Government actors have also become more assertive in developing their power over corporations. As mentioned in the above section, the Cyber Security Act 597 (Küberturvalisuse Seadus 597 SE in Estonian) introduced in May 2018 creates more formal requirements for corporations, making it compulsory to them to partake and submit cyber security auditing procedures and in following governmental standards.[860] Although these practices did occur in the past it was on an informal basis – the new act creates a more structured environment and moves governmental cyber security powers outside of just emergency and crisis-related legislation.[861] The Cyber Security act also enables Estonian Government actors to fine corporations that fail to comply. Estonian. In addition to legal constraints on their political power, corporations have struggled to assert influence through lobbying techniques.[862] Corporations have, however, largely accepted the new act.[863] Likewise, while the CDL was initially an ad hoc response to a crisis situation, the Estonian Government has since developed a more formal CDL structure. While the CDL is a civilian-based institution, it is nevertheless now placed within the territorial army. Despite this growing government capture occurring, these shifting dynamics have occurred in a highly stable environment. Several interviewees confirmed that corporations have broadly accepted the changes and understand the need for new regulation.[864]

The other area of evolution has been the growing role of international actors and networks, which, as the last section established, are able to become meaningful actors in an Estonian

[860] "Küberturvalisuse seadus 597 SE" (2018), https://www.riigikogu.ee/tegevus/eelnoud/eelnou/; Interview with Ministry of Economic Affairs and Communications Legal Advisor.
[861] Interview with Ministry of Economic Affairs and Communications Legal Advisor.
[862] Interview with Andres Kutt.
[863] Interview with Ministry of Economic Affairs and Communications Legal Advisor.
[864] Ibid; Interview with Andres Kutt.

cyber security context. Various international actors have sought to expand their remit to include cyber security and the long-term outlook of the role various organisations and networks will play remains unclear at present. As a small state with fewer resources, Estonia has naturally been a more active proponent of international cyber security cooperation. Similar to the growing role of Estonian Government actors, this process has so far been largely accepted – with Estonian Government actors often able to influence the agenda of target international organisations. Nonetheless, the simultaneous growth of Estonian Government actors alongside international networks and organisations could lead to tensions or disagreements in the future. However, the current track record would suggest that these two shifts are able to coexist happily.

The main potential source of instability within the Estonian Digital Society Assemblage stems instead largely from the novelty of digital society issues, as opposed to incentive divergences or rivalry between actors. With Estonia developing a variety of highly innovative yet often experimental digital society, initiatives – such as X-Road, digital embassies based abroad, and the KSI blockchain it is not yet clear how security provision will develop in these areas. The unfamiliar nature of many of these initiatives could lead to anticipated challenges. A variety of security experts have warned against online voting in elections for instance. The data embassy project has led to new questions about how policy and legal mechanisms can adapt to the issue at both an Estonian and EU level.[865] Although certain laws will be applicable, or at least compatible, with data embassies, it has also been realised that this may require modification to various domestic and EU laws and regulation.[866] Crucially, the scope of Estonia's Digital

[865] "Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government" (Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, 2015), https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.

[866] "Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government."

Society is expanding quickly as new schemes are launched. While this has not led to serious tension so far, it remains uncertain how these issues will develop in the future – and whether aspects of insecurity will emerge as a result. There is at least the possibility that the future nature of Estonia's Digital Society will present altogether new technical, political, legal and ideational questions – although the development of Estonia's Digital Society so far suggests that serious fractures are unlikely to occur.

It might be thought that privacy concerns present one area where tensions could arise between government actors and civilians going forward. Yet, privacy issues within Estonia have remained largely stable. As previously discussed, Estonia has a more open and transparent culture, where personal privacy issues are less sensitive than they are elsewhere. After over forty years of rule under the Soviet Union, many Estonians are proud to have their own institutions and this fosters a good level of trust according to Sikkut.[867]

Example One: Cyber security volunteerism

On the 2nd May 2007, Estonian authorities relocated a Russian war memorial from the central square in the capital Tallinn to a less accessible military graveyard in the outskirts of the city. The statue had become a sensitive issue – a symbol of the previous Soviet Union rule for most Estonians, yet a rallying point for Estonia's Russian-speaking minority.[868]

Although Estonian Government actors had anticipated a backlash to its removal,[869] the response from Russian hackers caught the country by surprise. What followed was a three-week campaign that included web defacements of political party websites carrying political

[867] Chambers, "Why Estonia Hasn't Built a Government Digital Service."
[868] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," The New York Times, May 29, 2007, https://www.nytimes.com/2007/05/29/technology/29estonia.html.
[869] ibid.

messages while both government and corporations found their networks targeted by sustained DDoS attacks. The targets included Estonian Government agencies, banks, schools, Internet service providers, and media channels.

Although DDoS and web defacements are nothing new, and widely regarded as unsophisticated forms of attack, they still had a decisive impact given Estonia's small size and high reliance on information systems and digital society infrastructure. Indeed, various government agencies were unable to send or receive email.[870] Banking services were also disrupted,[871] potentially leading to much great follow-on disruptions.

While CERT-EE directed the response to the attacks, the reaction nonetheless highlights the important role that cyber volunteerism plays in Estonia. Even though the CDL had not been created, the Estonian cyber security community in Estonia remained close, with strong links between corporations and Estonian Government actors. Three days after the initial attacks occurred, a number of Estonian civilian cyber security experts came together, including those working for Internet service providers, banks, police, governmental envoys, mobile telecommunication firms, and envoys from the government's Security and Information Boards.[872] An informal and ad hoc alliance formed to mitigate the impact of the attacks in a number of ways – for example, by supplying relevant appliances and hardware, filtering malevolent traffic, and providing information on the threat's scope, nature, and technical detail to the Estonian government.[873] By creating opportunities for collaboration, this informal alliance enabled different actors to work closely together in order to help overcome the unfolding crisis. The speed at which the informal ad hoc alliance formed in 2007 shows that

[870] Jackson, "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success," 2.
[871] Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* ed. Jason Healey (Vienna, VA: Cyber Conflict Association, 2013).
[872] Schmidt, "The Estonian Cyberattacks,"; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 193.
[873] Schmidt, "The Estonian Cyberattacks,"; Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 193.

civilian participation in defence is aligned with Estonian values and that this culture has transposed into a cyber security and digital society context.

The CDL has formalised civilian involvement in Estonian cyber security issues and a broader spirit of volunteerism has sustained. This is seen through the active role the CDL plays (as discussed previously) as well as the way corporations become involved in national cyber security issues. Indeed, one interviewee described corporations and the CDL as 'the same thing' (in reference to the emphasis on the cyber security community over actors).[874] The contribution of corporations in digital society security issues was also reflected in September 2017, when it emerged that there were serious concerns about the security of Estonia's ID card system in September 2017. Although not contracted out by Estonian Government actors, a variety of corporations nonetheless came together and volunteered their expertise and resources in order to rectify the problem,[875] reflecting both the harmony, but more critically of the high levels of hybridity in the Estonia Digital Society Assemblage.

Example Two: Estonia's Data Embassy project

The data embassy project refers to the Estonian Government's attempt to backup significant portion of its Digital Society initiative in the cloud. Data embassies house critical data registries and digital services,[876] ensuring the 'digital continuity', of e-Estonia in cases where the main

[874] Interview with Andres Kutt.
[875] Interview with researcher at Tallinn University of Technology.
[876] These include: State Budget Information System (Riigikassa Infosüsteem); Registry of Taxable Persons (Maksekohuslaste register); Social Security Register (Pensionikindlustuse register); E-File Registry (e-toimik); Land Register (Kinnistusraamat); E-Business Register (e-Äriregister); State Gazette (Riigi Teataja) – published all Estonian laws; Population Register (Rahvastikuregister); Identify Documents Database (Isikut tõendavate dokumentide register – UUSIS); Land Cadastre (Maakataster). See, "Suur Arhitektuurinõukogu," Riigi Infosüsteemi Arhitektuur, September 14, 2016, https://www.ria.ee/riigiarhitektuur/wiki/doku.php?id=an:kohtumised:140916; Lucas Kello, "Data Embassies: Consequences for National Security and State Survivial," unpublished manuscript, 2016. pp. 11-12.

data servers located in Estonia become unavailable.[877] This would mean, for instance, that portions of Estonia's digital society could continue to function in the event the nation was invaded. In addition to this opening up broader IR questions about whether a divisible form of sovereignty is now emerging that does not rely strictly on the control of a physical territory,[878] it also leads to more direct implications for the central research question and the hybrid nature of security provision, with both global-local and public-private distinctions blurred.

A component of Estonia's data embassy is hosted within Luxembourg although under the jurisdiction of the Estonian government.[879] Although embassies have long represented an extension of a state abroad, they have not previously enabled the continuity of key aspects of a state in the way the Estonian data embassy project promises. Ultimately, cyber security provision within a state is now inherently global. While this is typically due to the role of both multinational corporations and international organisations, data embassies also show that the global nature of cyber security provision also applies to government institutions as well. Crucially, critical elements of Estonia's Digital Society (which is becoming an increasingly integral part of the state) is now also based outside of Estonian territory.

Microsoft is also a part of the Estonian Digital Society Assemblage, involved in the data embassy project discussed in the Government Actors section above. In addition to both Estonian government clouds located in its borders, and the sovereign data centre located in Luxembourg, the Microsoft Azure cloud computing platform also plays an active role in ensuring the security and continuity of Estonian digital services. In 2014, measures were

[877] Interview with Mikk Lellsaar and Laura Kask (Ministry of Econimic Affairs and Communications employees) by the author and Lucas Kello. Tallinn, Estonia. April 26, 2017.
[878] Lucas Kello, "Data Embassies: Consequences for National Security and State Survivial."
[879] For instance, official of Luxembourg will be barred from accessing the data residing within the data embassy. See, Silver Tambur, "Estonia to Move Ahead With the 'Data Embassy' Concept," Estonian World, March 22, 2018, http://estonianworld.com/security/estonia-move-ahead-data-embassy-concept/; "Estonia to Open the World's First Data Embassy in Luxembourg," e-Estonia, June 2017, https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

developed to enable both the official website of the President of Estonia and the electronic State Gazette (Riigi Teataja), to be migrated and hosted on the Microsoft Azure cloud computing platform. Although these new and state announcement services might appear relatively unimportant in peacetime, they form a critical component of Estonia's digital continuity strategy, enabling an Estonian Government in exile to maintain an official communication channel with the Estonian public.[880] In this regard, a US-based technology firm is also a critical part of Estonia's Digital Continuity plans.

Security Outputs: individual security at the core

Both the configuration and dynamics of the Estonian Digital Society Assemblage have resulted in a highly stable and positive security outcome. Estonian citizens' personal data and privacy has yet to be severely compromised.[881] When there have been security concerns related to Estonia's Digital Society, the various security providers discussed have shown an impressive ability to organise and mobilise quickly in response to a threat or vulnerability due to the high levels of harmony and hybridity within the assemblage. Crucially, there is a single and shared view that exists across the vast majority of the assemblage, with a variety of actors striving for the same outcome without any clear conflicting objectives obstructing cyber security.

Given the convergence of incentive structures, as well as the harmony that exists between security actors, the broad distribution of power across the assemblage has been a good thing. While diffuse power distributions can be disruptive if different security actors disagree (creating the conditions of substantial power clashes), if security providers enjoy positive

[880] "Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government," 7.
[881] Priisalu and Ottis, "Personal Control of Privacy and Data: Estonian Experience," 447.

relationships then the assemblage benefits from a variety of actors with different pockets of expertise and perspectives work on security challenges together.

Hybridity has also been an important component of the high quality of Estonia's Digital Society protection. Although a variety of security providers comprise the Estonia Digital Society Assemblage, at least at the domestic level, the distinctions between these entities is highly fluid due to the high levels of fusion. There is a regular interchange of personnel between corporations and Estonian Government actors while a significant portion of those working for corporations in a cyber security capacity are simultaneously members of the CDL. All of this creates a highly agile response. For developing altogether new aspects of Estonia's Digital Society, it is appropriate for corporations to get paid given necessary investment of time and resources. Yet, if that same body of expertise is also able to assist Estonian Government entities via the CDL, the same individuals and pockets of expertise are able to be utilised in a variety of functions – all of which aid and contribute to the security of Estonia's Digital Society Assemblage. In this regard, the fusion of different domestic actors has enabled Estonian government actors to tap into expertise held elsewhere in a highly cost-effective manner.

Crucially, the variables studied in this thesis can also lead to highly positive security outcomes. In an Estonian Digital Society context, the traditional limitations inherent in small states are at least partially overcome. The positive harmony, the convergence of incentive structures, a broad distribution of power and the high levels of hybridity have all been influential variables in creating the conditions in which Estonia has been able to maximise its related security entities and direct them to keeping their digital society secure. This highlights the unique insight that can be gained through an assemblage approach.

Equally encouraging is the way in which individuals are actively considered within the Estonia Digital Society Assemblage. While civilians and individuals are an active part of the

assemblage through the CDL, Estonian citizens are also one of the core referent objects that the majority of security providers prioritise. In this regard, the democratic embeddedness of security is a high priority across the variety of domestic actors involved in the Estonian Digital Society Assemblage.

Estonia's Digital Society has been set up to empower Estonian citizens to keep government entities in check. Estonians are able to monitor how their data is accessed and used. X-Road enables different government-run databases to connect, meaning that a piece of data about an Estonian is only kept in one database.[882] It is this dual trust – Estonian government institutions developing secure systems while also in providing open and transparent digital society mechanisms that enable Estonians to understand how their data is used and secured – that sits at the heart of not only the ideational capacity of Estonian Government actors but also of the feasibility of Estonia's Digital Society more fundamentally.[883] Estonian citizens also have various powers and capabilities to both protect access to their data and to hold government actors to account. The political power of citizen is supplemented by The Estonian Data Protection Inspectorate that defends Estonian citizens' rights that include the right to obtain information about the activities of public authorise in relation to the data they access, the right to inviolability of private family life in the use of personal data; and the right to access data gathered about themselves.[884] In this regard, while there is a lot of data regarding Estonians citizens kept by Estonian government databases associated with their digital society,[885]

[882] "X-ROAD: A Secure Data Exchange Layer for Building e-Governments."
[883] Priisalu and Ottis, "Personal Control of Privacy and Data: Estonian Experience," 443.
[884] Statute 44, "The Constitution of the Republic of Estonia" (1992), https://www.riigiteataja.ee/en/eli/521052015001/consolide; "Personal Data Protection Act" (2008), https://www.riigiteataja.ee/en/eli/509072014018/consolide; "Inspectorate," Estonian Data Protection Inspectorate, November 22, 2017, http://www.aki.ee/en/inspectorate.
[885] This includes their name, date of birth, gender, address history, citizenship, and legal relationships, the land they own, mortage details and political part membership. See, Peter Herlihy, "Government as a Data Model': What I Learned in Estonia," Government Digital Services, October 31, 2013, https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/; Estonian Government employee, interviewed by Jamie Collier, Tallinn, Estonia. February 11, 2016.

Estonian citizens can actively monitor who is accessing their data. The Estonian Data Protection Inspectorate also ensures government entities are accessing data appropriately as according to existing laws and regulation but also help to draft new policy and are act as a law enforcement agency with powers to fine those who access data in the Estonian Digital Society inappropriately. Access controls also limit inappropriate intra-agency access – a traffic police unit would not have access to the breadth of criminal cases that a detective would be able to see for example[886]. In addition to fines, Estonian government employees can also get fired and there is even the possibly of criminal cases for unreasonable access.[887]

Privacy standard are highly relative across the world and the ideational capacity of Estonian Government actors also hinges on Estonia's highly open culture (in line with Nordic societies).[888] Openness is often emphasised in the official documentation of the Estonian approach, originating as a reaction against the closed nature of the Soviet regime from which modern Estonia emerged.[889] Although some databases run by Estonian Government entities are kept confidential and guarded by strict access controls, there is also a great deal of information freely available for anyone in Estonia to look up including general information about an individual's mortgage, their political party membership, and land ownership records.[890] Estonians take a more relaxed approach[891] to these issue with the privacy from government entities a less sensitive issue when compared with other cultures. For example, while being a political party member is regarded as a private matter in the UK, in Estonia it is regarded as a pubic endorsement[892] – it would therefore be nonsensical for such information to be kept

[886] Interview with Estonian Government employee, interviewed by the author. Tallinn, Estonia. February 11, 2016;
[887] ibid.
[888] ibid.
[889] Margetts and Naumann, "Government as a Platform: What Can Estonia Show the World?"
[890] Interview with Estonian Government employee.
[891] ibid.
[892] ibid.

confidential.[893] It is this more open culture, and the subsequent lack of sensitivity over the privacy of certain information, that means Estonians are relatively comfortable with Estonian Government actors having a prominent role in the Estonia Digital Society Assemblage.[894] In this regard, despite the significant amounts of data stored on Estonians (that comes with digital society initiatives) this is not perceived to have undermined Estonian privacy, given their more open culture.

With civilians a significant component of Estonia's Digital Society, they also receive positive ideational support. Jaan Priisalu and Rain Ottis have argued convincingly that civilians must not only trust government entities, but government entities must also trust civilians for Estonia's Digital Society to function effectively.[895] If Estonians failed to engage with digital society platforms or inputted incorrect data into these systems, the whole process would be undermined.[896] Yet Estonia's Digital Society Assemblage assumes a level of goodwill to cooperate and contribute in a positive manner.[897] Indeed, the Estonian Digital Society Assemblage shows the benefits that can be derived from a truly 'whole of nation' approach to cyber security.

Estonia Digital Society Assemblage Chapter Conclusion

An assemblage approach has been essential in empirically capturing Estonian cyber security provision. Out of all three of the cases studied, Estonia has exhibited the highest levels of fusion in a security structure. Traditional ontological barriers between actors are increasingly blurring with different security providers often working together as a community. Given such a reality, it inherently makes sense to study this social structure through a theoretical approach that is

[893] ibid.
[894] ibid.
[895] Priisalu and Ottis, "Personal Control of Privacy and Data: Estonian Experience," 444.
[896] ibid., 444.
[897] ibid., 444.

capable of not only accommodating hybridity, but also one that explores what it means for security provision.

This chapter has shown that that not only do a combination of diffuse security actors provide security in Estonia, but also that cyber security is a challenge where non-traditional units including volunteer and civilian groups can play an important role. Domestic actors play a prominent role in Estonia's Digital Society Assemblage and the close links that exist in a small state as well as the overlapping of different units and actors have fostered significant levels of fusion. This was shown most clearly with the same individuals often simultaneously part of a corporation and the CDL. Positive domestic dynamics have been supplemented by the countries inclusive and welcoming posture towards international organisations. Given Estonia's focus on technology and related fields, the country can make an outsized impact on digital and cyber security policy within larger organisations such as the EU. In this regard, while international organisations supplement the protection of Estonia's Digital Society, they are also a platform for Estonia to project power and influence. Here, an assemblage approach considers how actors reassemble and reform in the face of globalisation and emerging security challenges. As cyber security has emerged, different international organisations have sought to frame themselves as relevant security actors. With Estonia providing a particularly welcoming environment for international organisations pursuing a cyber security remit, these processes of international organisations reforming themselves and seeking to promote their own cyber security remit discussed through an assemblage approach has provided a useful framing for understanding how international actors are responding and adapting to emerging security issues.

With civilian actors playing an important role and arguably due to Estonia's small size, the security outputs within Estonia's Digital Society Assemblage closely reflect the interests of

individuals. In this regard, traditional IR approaches focused on power and interests provide limited value in explaining Estonia's digital society security outcomes. Instead, an assemblage approach that considers the harmony between actors and their connection to Estonian society as a whole has been central in understanding the state's security outcomes.

The Digital Society project as a whole is largely dependent on trust and buy-in from Estonian citizens. This symbiotic relationship between security providers and citizens has created both harmonious dynamics and largely positive security outcomes.

Chapter Six: Conclusion and the Case For Studying Cyber Security Provision

Thesis Findings and Core Arguments

This thesis has sought to understand how the complex configuration of security actors, and the dynamics that exist within security structures, influences the provision of cyber security. This is a question that cannot afford to be neglected, given the fundamental implications it has on both national and individual security. The ambition of this research has been to build up a more robust body of evidence that highlights why security provision issues are as important to consider as other drivers of cyber insecurity.

The theoretical model outlined in Chapter Two provided a conceptual framework that allowed issues of cyber security provision to be explored in depth, breaking down the often loosely defined assemblage term into two overarching concepts: Assemblage Configuration and Assemblage Dynamics. Assemblage Configuration captured the relevant security providers within an assemblage, as well as their incentive structures and power. Assemblage Dynamics then moved beyond mapping actors and explored the processes occurring in a security structure – the level of cooperation and the type of relationships that exists between different security actors; the extent to which different actors were becoming amalgamated; the areas of contestation; the development of these factors over time; etc. Again, specific variables – including harmony, hybridity and evolution – were used to capture dynamics in a more refined way. In doing so, this thesis has made an argument for examining contemporary security issues through an assemblage approach, given the unique insight it provides through examining issues

and variables (as mentioned above) that are too often neglected within IR and security studies, despite their influential bearing on security outcomes.

This conclusion will tie together and integrate the arguments and research findings covered in previous chapters. However, it is first useful to briefly outline and recap the specific findings of each case study individually. Here data gathered through interviews, other primary sources (including legal documents, and speeches), as well as various secondary sources was used to develop an in-depth understanding of the security actors that reside within the assemblages studied, and the dynamics that exist within these social structures.

The US Encryption Assemblage examined in Chapter Three uncovered a security structure fraught with tension and contestation. Two mutually exclusive visions of security clashed fundamentally. The Assemblage Configuration section showed there was a significant degree of complexity in the assemblage, given the broad distribution of power and the variety of incentive structures held by security actors. The combination of these variables created much of the disruption observed in the Assemblage Dynamics section. There was a significant lack of harmony – most clearly observed through the disputes between strong and weak-encryption clusters, but also highlighted though the divisions that existed within each of these inter-unit clusters and within traditional units (most notably within the US Government). These divergences showed that the traditional framing that characterises encryption debates as a dispute between either privacy and security[898] or between the US Government and the private sector[899] are overly simplistic and obscure many of the practices and dynamics observed. The high levels of fragmentation naturally led to a highly combative assemblage dynamic with few

[898] Kevin Anderton, "Privacy Versus Security; How Americans View the Issue of Encryption," Forbes, February 16, 2017, https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/kevinanderton/2017/02/16/privacy-versus-security-how-americans-view-the-issue-of-encryption-infographic/.
[899] Sara Sorcher, "The Battle between Washington and Silicon Valley over Encryption"; Shanika Gunaratna, "The Snowden Effect: Silicon Valley vs. the Government."

instances of fusion or cooperation between actors. The impact of these variables was then examined through an examination of security outcomes. Here, no actor or side of the debate has been able to achieve a sustained level of dominance, making the evolution of the assemblage unstable. A constant iterative process is therefore occurring: encryption is undermined by weak-encryption actors before being corrected by strong-encryption actors with the process then repeating. This is largely caused by the lack of fusion on either side of the debate. The US Encryption Assemblage therefore has an inconsistent and constantly changing state of data security, with individuals finding themselves largely unrepresented by the various stakeholders involved.

The UK CNI Assemblage was then explored in Chapter Four. The Assemblage Configuration section again highlighted the variety of security actors, yet power was largely centred within corporations (who own and manage the majority of UK CNI).[900] An overview of corporations also showed the breadth of actors that exist – ranging from local not-for-profit companies to large multinationals and state-owned or quasi-state firms. While all security actors want theoretically the same thing – a secure CNI infrastructure – it has been argued that a market failure exists with profit-motivated actors underinvesting in the issue.[901] Yet, despite UK Government actors criticising corporations (in both public statements by key policymakers and in official cyber security strategy documents), this discontent has not led to significant tension. A variety of shared practices and overlapping infrastructure has led to a significant degree of hybridity between UK Government actors and corporations with a public-private partnership cluster highly prominent in the provision of security. This level of fusion has made it difficult for UK Government actors to challenge the role of corporations. While underinvestment in cyber security has not led to significant security failings so far, the long-term implications

[900] Ashford, "Is UK Critical National Infrastructure Properly Protected?"
[901] Sam Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security."

could lead to negative outcomes for individuals given the increased digital dependence of the UK economy.[902]

The Estonian Digital Society Assemblage analysed in Chapter Five provided a view into a highly advanced digital economy that is experimenting with new and innovative projects. The Assemblage Configuration showed the cyber security of Estonia's Digital Society was also provided by a wide breadth of actors – including a prominent role for civilian volunteers. Similar to the UK CNI Assemblage, a significant degree of the technical capability within the assemblage resided with copromotions. Yet, the Estonia Digital Society Assemblage stood out with the vast majority of actors' incentive structures more closely aligned. This led to positive assemblage dynamics with healthy relationships between the different security providers. The characteristics of Estonia also meant the assemblage was welcoming of international networks and organisations taking on a greater role. The overlapping incentive structures at the domestic level has led to significant degrees of hybridity, with the distinctions between civilian groups, corporations and government actors highly blurred. There is instead more of an emphasis on the Estonian cyber security community at large – an interunit cluster that works very closely together. The positive dynamics have also led to a very stable evolution over time – even in instances where the Estonian Government has increased its power over corporations. This all leads to a positive security output with the security (and broader interests) of individuals firmly baked into security provision practices.

The link between the characteristics of security structures and the nature of security provision is axiomatic. More useful insight, therefore, comes from further breaking down the notion of security structures (or assemblages) into a set of more refined concepts and variables that can

[902] "Government Digital Strategy" (London, UK: HM Government, November 2012), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf.

be studied in a with greater precision. The theoretical model and conceptual framework outlined in Chapter Two facilitated such a discussion. Here, it becomes clear that the majority of the variables studied are not on their own definitive of a particular outcome. For example, neither a broad distribution of power nor a highly harmonious assemblage necessarily leads to a predictable security output. This is unsurprising: the sheer complexity of the assemblages studied mean a single variable is unlikely to be significant on its own. It is instead necessary to consider a number of variables in combination.

The one variable that stands out the most when examined on its own is the incentive structures of security actors (and the extent to which the various incentives held by different security providers converge). The US case study showed that assemblages that comprise actors with radically opposing, and mutually exclusive, visions of security are likely to result in an assemblage dynamic fraught with tension and disharmony (and one that ultimately impacts individuals given the competition between securities). The US case study also revealed the insights that can be derived from exploring incentive structures in substantial depth: while the main source of dispute exists between strong and weak-encryption actors, the tensions that exist within both of these camps also leads to an even greater level of tension and ultimately a lack of fusion (with different actors that share a mutual interest in either strong and weak-encryption still often competing or unable to fully cooperate with one another). The UK case study also revealed the importance of exploring incentives in depth. The vast majority of security actors want the same thing (a secure CNI) and there are not the fundamental clashing securities that were observed in the US case study. However, despite this shared interest theoretically, a number of actors diverge in practice. With security one of a number of priorities, it naturally competes with other objectives (including a desire to reduce costs). It has therefore been argued that a cyber security market failure exists, with official UK Government strategy accusing market forces of failing to produce the optimal level of cyber security

investment.[903] Government actors have shown they are not immune to this trend either with the spread of the WannaCry ransomware highlighting a lack of IT investment in government-managed UK CNI. As for Estonia, the shared incentive structures of the various security providers have created significant harmony and hybridity given the extent of cooperation. This has also led to positive levels of cyber volunteerism with both citizens and corporations contributing to the broader security of Estonia's Digital Society (often in an unpaid capacity). Further, with the concept of digital society regarded as a fundamental aspect of the nation, the interest and rights of individuals have been integrated into security provision. It would therefore appear, based on the three case studies, the extent of compatibility between the incentive structures of different security providers is a significant factor in determining the hybridity and harmony of an assemblage, as well as the broader stability of security outputs, and the extent to which it is corelated with the interests of individuals.

Despite the divergences between each case, all three nonetheless contain a significantly broad distribution of power between security actors, highlighting the power diffusion process that has occurred in various cyber security contexts. While certain actors may dominate more than others, no case study displayed anything that even closely resembled a unitary security actor. This reaffirms the importance of examining cyber security as provided by a diffuse network of actors. The broad distribution of power is perhaps most notable in the US case. With both strong and weak-encryption clusters possessing a meaningful capability, neither side is able to dominate the assemblage. The broad distribution of power therefore compounds tension and leads to an iterative and unstable security outcome, where the encrypted data of US citizens is sometimes accessible by weak-encryption actors while at other times remains secure. The UK CNI Assemblage, by contrast, is largely dominated by corporations and this has proved a

[903] Sam Jones, "GCHQ Chief to Say Free Market Failing on Cyber Security."

significant factor in sustaining a situation where UK Government actors have struggled to appropriately intervene. The standing of corporations is reflected through the presence of highly controversial foreign-based firms who have enjoyed a prominent role in the assemblage, despite being barred from government contracts in other Western economies including the US and Australia. The Estonia Digital Society Assemblage has a more diffuse distribution of power and while corporations possess the majority of skills, expertise and talent, Estonian Government actors have nonetheless grown in prominence and gradually developed a more assertive stance.

The broad distribution of power across multiple security actors has both positive and negative implications. In many ways, this fosters healthy security dynamics. This is because different actors within an assemblage have the capability to serve as a check and balance against each other. No security provider discussed in this thesis enjoys an unbridled ability to establish its own aims and ambitions when they are opposed by other security actors. The broad distribution of power has therefore prevented any one threat actor, and its vision of security, from becoming too dominant. This was most clearly shown in US encryption disputes, although it is also clear that the Estonian Government is only able to fully pursue its vision of security as it is aligned with other Estonian security actors as well as Estonian society as a whole. Again, this highlights the strength of an assemblage approach due it focus on variables including hybridity and harmony that directly impact security outcomes.

Whilst it is a broadly positive outcome that these dynamics prevent any actor from enjoying unparalleled power, the broad distribution of power can also inhibit optimal security outcomes. Each security actor typically pursues its own self-interest; checks and balances then occur as the aims and incentives of security actors deviate. Clashes are therefore primarily driven by narrow self-interest, as opposed to a desire by security actors to secure the referent object of

each case study or ensure that the democratic embeddedness of security is achieved. Of course, assemblages often reflect the makeup of the society that they represent. Tensions between actors in the US Encryption Assemblage at least partially mirror tensions over the issue within American society. Yet, societal views on optimal security outcomes are ultimately imperfectly aligned with the security outputs that arise through the assemblage dynamics studied in this thesis. The power of corporations discussed in the UK CNI assemblage means that government checks are arguably too weak to fully correct a market failure. Although technology firms may appear to be a natural check on the weak-encryption vision of security pursued by law enforcement that is aligned with the portion of American society that prioritises privacy, these firms are not meaningfully representing this portion of the US while they simultaneously commercialise user data in a way that many privacy advocates contend. Crucially, power is not democratically distributed within cyber security structures. This makes an assemblage approach that studies how roles are constantly shifting and being redefined a highly useful conceptual and theoretical tool for understanding nascent security issues given the regularly shifting nature of early security structures.

While a broad distribution of power exists most clearly in both the US and Estonia, both assemblages have altogether different security outputs. This shows that while important, the distribution of power is not decisive in isolation.

A similar observation is found when harmony and hybridity are examined. While the most positive security outcomes are observed in the Estonia Digital Society Assemblage (where hybridity and harmony are at their highest) and the most unstable and disruptive security output is observed in the US Encryption Assemblage (where hybridity and harmony are at their lowest), this does not mean that hybridity and harmony alone determine an assemblage's security output. Indeed, the UK provides an interesting example, where the high levels of

hybridity (as observed in the various practices that occur within the public-private assemblage cluster) constricts government actors from fully challenging the role of corporations. Crucially, the UK example suggests that, at times, disputes and tensions between security actors might in fact improve security outputs and correct misaligned incentive structures. High levels of fusion, while positive in the Estonia case, arguably restrict the UK. The Estonian example also shows the positive influence these factors can have on security provision. As a small state with minimal resources, Estonia has been able to maximise the security of its Digital Society through a hybrid structure where various actors work together on what is largely a shared mission. Crucially, however, this thesis has highlighted that these variables that linked to an assemblage approach matter and can directly impact security provision

An analysis of the variables studied therefore highlights the complexity of contemporary cyber security structures. It is the combination of variables that actually matters. In the US case study, the variety of clashing incentive structures is made meaningful when combined with the broad distribution of power, (which enables both strong and weak-encryption actors to build up capability), creating the conditions for tension, disharmony and iterative security. In the UK case study, the incentive for corporations to underinvest in cyber security is significant when combined with the significant levels of fusion between public and private actors, thereby entrenching UK Government actors into partnership structures that make it difficult to challenge corporations.[904] As for Estonia, the shared notion of protecting the country's digital society infrastructure, has combined with the high levels of hybridity and harmony to create a highly positive security output.

There is a need to reorient cyber security studies towards a more serious focus on security provision: the actors that provide security, their incentive structures and capabilities, and the

[904] Of course, the Government is also arguably incentivised to refrain from intervening anyway. See, Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies."

way different security actors interact. It is also vital to study security structures given that their dynamics are constantly changing and due to their often highly unstable dynamics. This thesis has identified a variety of important trends and processes that highlight the diachronic nature of security provision. Government actors are often portrayed as latecomers to cyber security, albeit often unfairly. Yet, cyber security is becoming increasingly prominent on policymaker's agendas with governments now significantly investing in the issue. Whilst it is true that aspects of cyber security governance have long been a private sector remit, government actors are rapidly becoming more dominant and assertive players (and were also highly influential the initial development of the Internet). Across all three case studies, the fluid and shifting nature of power represents a perennial theme. This is most clearly observed in US encryption disputes, yet the UK Government public challenge on the flaws of a market-led approach to cyber security,[905] and the expansion of the Estonian Government's powers through new laws[906] both show that the balance of power is rarely static in cyber security contexts.

Various perils accompany shifts in security provision. As government actors become increasingly involved in cyber security, there are real prospects that the issue will become further securitised. Both NATO and domestic military departments risk over-militarising cyber security and what should often remain a civilian issue.[907] Crucially, there are a number of ways that cyber security can be presented (whether that be through a military, crime, or intelligence framework, etc) and the growth of actors and the narratives that they push forward can reinforce or undermine certain visions – all of which have implications for the security outputs affecting individuals.

[905] "National Cyber Security Strategy 2016-2021," HM Government.
[906] "Küberturvalisuse seadus 597 SE" (2018), https://www.riigikogu.ee/tegevus/eelnoud/eelnou/.
[907] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better"; Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension."

Both the UK and Estonia case study made it clear that international actors and networks are also keen to expand their cyber security remit. This should largely be welcome, with more robust international frameworks offering a prospect for improving cyber security. However, there is also potential for international institutions to become overly involved, or for the space to become crowded and thereby create inefficiencies. Although often necessary, the replication of services and arrangements (either both at the domestic and international level or between two international organisations) often leads to a wasteful allocation of scarce resources. Crucially, whether in a domestic or international context, it is vital that questions of delegation and an understanding of how the different portions of cyber security remits are divided require careful consideration.

With the variables discussed throughout this thesis (including incentive structures, hybridity, harmony, and the distribution of power) shown to have a highly influential affect in determining security outputs, the findings of this thesis also touches on issues related to the agency of security actors themselves. This thesis poses a question related to the extent to which security outputs are determined by these variables independently, or whether security actors can themselves have an influential bearing on security outputs notwithstanding the configuration and dynamics of an assemblage. Here, it is immediately clear that presenting these two perspectives as a straightforward binary choice is unhelpful given that aspects of both perspectives apply.

The variables discussed clearly influence security provision and create a certain degree of path dependency. The UK government has limited ability to change the course of its interaction with corporations, given the levels of fusion and entrenchment of public-private partnerships for example. Likewise, law enforcement actors and technology firms in the United States are unlikely to significantly alter their vision on encryption, given their institutional incentives.

At the same time, however, security actors are clearly not exclusively ruled by the levels of hybridity and harmony. With this thesis having considered security actors' incentive structures, the agency of these actors is already baked into the conceptual framework used to some extent. Yet, an actors agency goes beyond their incentive structures. The individuals that make up a security actor confront decisions on a daily basis on how they navigate assemblage dynamics. This would include the extent to which they are willing to compromise on an issue; the tone in which they enter into interactions, negations, and bargaining with other security actors; the way actors respond to contentious decisions and actions; etc. Ultimately, despite the constraints established by these variables, there remains room for manoeuvre where security actors and individuals have meaningful agency to affect the future outcome of an assemblage.

The interplay between the variables studied in this thesis and the agency of security actors and individuals mean it is essential to study the evolution of an assemblage over time. Security assemblages are in constant motion, with both their configuration and dynamics often changing over time. Rather than statically looking at how hybridity and harmony affect security outcomes, this thesis has explored how security actors react to these dynamics, as well as how these reactions alter this very dynamics and how this in turn impact security outputs.

Implications for Theory and Practice

The findings of this thesis contain both practical and academic implications.

While this thesis has not dwelled on the relevance of state-centric paradigms, the findings nevertheless highlight the complex configuration of cyber security structures. While traditional state-centric IR theories still have much to offer, it is crucial to also recognise where they fall short. Of course, this insight is not particularly new or controversial. Buzan has shown that the units, systems, structure and process that have characterised much of IR do not apply to various

time periods and regions when a broader world history is considered.[908] It is self-evident that as a more simplistic framework, state-centric paradigms will not capture the level of nuance of an assemblage approach and this is neither inherently good or bad – they are simply different types of thinking tools that are more or less useful depending on the subject and level of nuance required. Crucially, however, this thesis has shown the insights that can be achieved by going beyond questions of whether contemporary security structures (or assemblages) are compatible with state-centric theories and concepts. What is interesting about the case studies examined is not in understanding where such traditional theories fall short, but in uncovering the sheer complexity of security provision and how assemblage thinking offers a means for understanding such dynamics.

Despite the focus on security provision, the findings of this thesis still contain important implications for IR theories and concepts about agency and sovereignty in international affairs. The critical point is not that states have become weaker in a cyber security context (although this is arguably often the case) but that states operate within a broader network that often have high levels of interdependence. Governments bring in various actors through outsourcing and partnerships that are a critical component of their capability. The implications of these diffuse structures go beyond issues of interdependence. A government's agency is to some extent determined (and often limited) by the networks or assemblages it exists within. Other security actors that are also part of these networks can both complement or undermine a government's objectives. A key aspect of a government's manoeuvrability therefore depends on how they navigate these diffuse networks. It is therefore vital for IR and security studies to further accommodate the issues and variables that are examined through an assemblage approach.

[908] Barry Buzan and Richard Little, "Waltz and World History: the Paradox of Parsimony."

An important finding of this thesis is in reaffirming the insight that can be derived from reorienting security studies from an examination of traditional units to that of individual actors – as has been discussed through other approaches including Actor Network Theory. All three of the case studies have shown that traditional units rarely represent a coherent and uniform whole. The UK case study demonstrated that a range of actors reside within a traditional unit – an analysis of corporations ranged from not-for-profit corporations, to UK-based firms, to multinational corporations and quasi-state corporations. US encryption disputes have likewise highlighted the internal division that exist within the US Government. The Estonian case study showed how a variety of international organisations are seeking to capture the cyber security remit, often with contrasting approaches based on their institutional culture. The different motivations and characteristics of actors that sit within traditional units was articulated through intra-unit clusters – such as profit-motivated corporations in the case of the US Encryption Assemblage or the intelligence community in the UK CNI Assemblage. Yet, even within such intra-unit clusters there is further complexity (and further divisions). The NSA, CIA and FBI are very different organisations despite all being part of the US intelligence community; Apple's business model based on selling products contrasts starkly with other profit-motivated corporations such as Facebook and Google that primarily generate revenue through monetising user data. Security studies can therefore benefit from further accommodating the individual and often unique agency of specific actors, with traditional unit-oriented study often blunting crucial understanding.

This thesis has also demonstrated the ways in which security actors are significantly changing. In part, this is related to the emergence of non-traditional actors – whether that be the Cyber Defence League in protecting Estonia's digital infrastructure, or the role of liberal academic centres in questioning the merits of weak-encryption policies. Indeed, while power diffusion processes are often explored through a threat lens, it also leads to new security providers

becoming increasingly relevant. When it is considered that many of the most serious cyber attacks have still emanated from states, power diffusion processes have the most serious implications for security provision.

It is not just non-traditional actors coming to the fore – the role of traditional actors and units are also shifting. The private sector, in many cyber security and technology contexts are now no longer just selling goods and services. They are increasingly forced to go beyond their traditional role and thrust into profoundly ethical, strategic, and foreign-policy challenges. Apple no longer just sells phones and laptops but is a guarantor of security and privacy. A government's standing as the default security provider in cyber security is by no means guaranteed; instead they must compete with others to sell their notion of what cyber security means to the public. This notion of competition within a security structure is central to an assemblage approach.

Security actors and practices often transcend public-private and global-local distinctions. While each of the three case studies focused on a domestic referent object, they all nonetheless contained a variety of actors and entities that lied beyond their national borders. The role of the National Grid in the UK CNI Assemblage provides a case in point: it is heavily involved in UK CNI and thus interacts very closely with UK government actors,[909] thereby blurring public-private distinctions while it is an organisation based in both in the UK and US with cyber security staff working to secure both geographies, thus also transcending global-local distinctions.

Distinctions between actors and units are also often blurring in the face of emerging fusion – a feature essential to assemblages. The entire Estonian cyber security community works together

[909] Interview with National Grid employee.

to protect Estonia's Digital Society.[910] Cyber security employees from the private sector are embedded in the UK Government's NCSC.[911] These practices should not always be portrayed as forms of cooperation or partnership – that would imply two wholly ontologically distinct actors working together. Instead, different actors regularly become entwined and embedded with one another within assemblages.

At a practical level, the findings of this thesis help explain the reality of security assemblages and to distinguish between public narratives and realities – issues highly relevant to public policy. As previously mentioned, technology firms often claim to develop strong-encryption as a means to protect user privacy, yet such a position is hard to justify in reality given the scale at which they simultaneously monetise user data (thus suggesting they are at least partially promoting strong-encryption as a way to distance themselves from government actors and to protect their brand).[912] The theoretical model in this thesis, with a focus on incentive structures helps to understand the alternative explanations for the actions of security providers.

Any security provider must therefore consider both their own incentive structures and those of other actors that they interact with. With the case studies highlighting that there are often a variety of different and sometimes competing incentive structures within government, it is vital for public policy to grasp these potential tensions. Where conflict does exist, procedures and mechanisms that appropriately balance conflict should be implemented. For example, the US Government would benefit from establishing central committees and processes comprising the various governmental stakeholders on encryption. Here tensions and policy disagreements

[910] Interview with Andres Kutt.
[911] "Industry 100," NCSC, March 19, 2018, https://www.ncsc.gov.uk/information/industry-100-faq.
[912] Mark Hachman, "The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers."

could be presented and weighed against each other, ideally under the supervision of elected officials.

An understanding of the concepts and variables discussed in this thesis, and how they link together, also provides insight for designing better and more efficient security structures. To make improvements to security structures that are disharmonious and fragmented, it is first necessary to fully establish how such dynamics have arisen. The Estonia example shows the benefits that can be derived from an assemblage where there is a clear sense of a shared mission between security providers (an important takeaway for other small states with a similar culture). Although this might not be possible in other contexts and for larger states, it nonetheless represents a useful case study for how a government can engage with other stakeholders in a highly productive manner. The case studies also highlighted the importance of missions and remits being clarified early on. The UK and US cases highlighted the internal divisions that can exist within governments for example. In the UK however, many of the disputes and internal rivalries have been at least partially resolved through the creation of the NCSC, which has gone a long way in developing a coherent entity that represents the UK Government as a whole. Although there are benefits to a decentralised governmental response, where inefficiencies or departmental rivalry over ownership of the cyber security mission arise, there is a compelling case to create more centralised bodies such as the NCSC.

With both the referent object and country not held constant across the case studies, the generalisable findings of this thesis are naturally more constrained when compared to positivist projects focused on establishing causal mechanisms. With generalisable findings often the yardstick used for measuring IR research, the key findings outlined above could therefore be criticised for not going far enough. Yet, there are numerous ways in which this thesis does make a clear contribution to IR and security studies.

First, the findings of this thesis do provide generalisable insights. While not formal causal mechanism per se, this thesis advances knowledge about both cyber security provision and the application of assemblage models. From a cyber security perspective, the case studies have empirically demonstrated the highly diffuse nature of cyber security structures. While the implications are different for each case, this thesis has nevertheless highlighted that the configuration of security structures has fundamental implications for security outcomes – a factor too often ignored when exploring drivers of insecurity. Hybridity is a concept rarely considered as a mechanism that seriously impacts security, yet this thesis has shown that it is an essential attribute to consider. It has also been argued that both public-private and global-local distinctions are eroding across a variety of cyber security contexts. The findings of this thesis also show how the core principles underpinning assemblage theories apply to cyber security, a topic that has not seriously been explored from an assemblage lens before. It shows how an assemblage theoretical framework can be highly relevant in examining emerging technological issues. All of this shows that while this thesis has not identified strict causal mechanisms, it remains an ambitious project that provides broader forms of generalisable findings that are equally valuable.

Second, this thesis has provided both a conceptual framework and relevant variables that provide a foundation to go on and develop more formal generalisable findings. Further research could compare the same referent object across a range of states, examining how more or less hybrid assemblages react to the same issue. Likewise multiple security topics could be studied uniformly across a handful of states. A study could, for example, study both encryption as a contentious topic and CNI as a more stable topic across multiple assemblages that range in size, hybridity, evolutionary structures, etc. All of these research endeavours would provide further and more specific insight into how the variables studied in this thesis interact and produce security outputs. While this could be read as a criticism of this thesis for not taking on

such a project, it is only possible to arrive at this critique once the exploratory work of this thesis has been achieved. Crucially, it would not be possible to know how these possible research projects could have been structured if this thesis had not demonstrated the importance of the variables studied related to the configuration and dynamics of an assemblage structure.

Third, this thesis has often focused on a different type of research, meaning generalisable findings are ultimately not the only litmus test that should be applied. Explorative research instead provides insight by through rich and nuanced understanding of the subject matter. This thesis has explored cyber security provision, a topic relatively underexplored in cyber security literature, and brought attention to emerging cyber security processes that are important in themselves. Issues such as public-private entrenchment; the fracturing of government entities on issues such as encryption; and the blurring of national boundaries within digital society infrastructure all pose significant implications for cyber security. These trends have been neglected, yet by explaining

Finally, the findings of this thesis can be used to forecast potential risks and fallouts. While partnerships between actors are often vital, the UK case study nonetheless highlighted the risks of building hybrid structures and security practices – for example, by preventing governments from appropriately challenging and holding corporations to account. If, as in the US case study, it is clear that different security actors have fundamentally opposing incentive structures, this is highly likely to become a source of tension, therefore reaffirming the need for early dialogue and the building of relationships in order to at least explore how compromises might work and how differences might be coexist in a way that builds stability and an outcome mutually acceptable for all parties (including individuals). Not every actor has complete agency on how relationships and assemblage dynamics will formulate. Yet, by being aware of the likely

outcomes, they can at least become more proactive in engaging and seeking to mitigate the disputes most likely to arise.

Future Research and Conceptual Avenues

This research project has provided new exploratory insights. The main intention was to identify and propose variables related to security provision that could have implications for security outputs. Having shown the relevance of the key terms discussed throughout the thesis, there is now an opportunity to further explore these issues though more formal theory testing IR research projects. This could, for example, involve looking at one of the three security topics in further depth. The variety and divergence of cases in this thesis enabled a broad study, yet there would also be benefit in now focusing on a variety of countries and examine the differences in how they deal with encryption, CNI or digital society initiatives. With a security topic fixed, it would then allow for a more substantial cross-case comparison and the opportunity to derive more substantial causal claims.

The specific variables could also be explored in further depth. From a public policy perspective, there would be benefit in examining a variety of assemblage structures where opposing incentive structures exist. Research could then explore out of all such cases, where conflict, tension and negative security outputs are most prominent compared to where assemblages have been able to manage and even mitigate disagreements in a more productive manner – providing lessons for how divergent incentive structures can be better managed and accommodated within security structures. It would also be beneficial to further explore the notion of hybridity – both in how it differs across a range of case studies and also to further understand the implications that various forms of fusion have on security outputs. As the above section outlined, apart from incentive structures, the variables studied were rarely influential on their own – instead it was the combination of multiple factors that led to security outputs. Further

studies could therefore further explore these combinations. It is here, that there is the most promising potential in developing causal mechanisms.

The Estonia Digital Society Assemblage also uncovered further variables that appeared significant and deserve more analysis in their own right. As a small state that operated a total defence model (where there is a culture of civilian involvement in defence), alongside a compulsory national service period, Estonia arguably enjoyed advantages that other states would be unable to capitalise on.[913] Yet, the extent to which this is a universal rule remains to be seen. Further research on the cyber security response of small states would therefore yield useful findings regarding the extent to which such security models can be exported into cyber security contexts – as well as provide broader lessons on power diffusion and the roles that small states can play in cyber security.

For all their differences, the three case studies in this thesis nonetheless were all modern Western economies with a high level of cyber security maturity. Yet, thinking with assemblages, and applying the variables discussed throughout this thesis offers great promise in different contexts. Assemblages are naturally suited to explore structures that are inherently international – internet governance provides a good example of this, with a global and multi-stakeholder approach at its core.[914] Likewise, the developing world presents radically different cyber security structures. In autocratic regimes, the state is not always a security provider and might even represent the primary threat for individuals. Understanding the various non-state actors that mobilise to provide cyber security – often in response to threats emanating from the government – would be a phenomenon that would be fascinating to explore though an

[913] Interview with Ministry of Economic Affairs and Communications Legal Advisor; Areng, "Lilliputian States in Digital Affairs and Cyber Security."
[914] Madeline Carr, "Power Plays in Global Internet Governance."

assemblage lens. There would also be clear benefit in studying states including Russia and China with assemblages, given the naturally blurrier lines that exist between governments and other institutions.

From an IR theory standpoint, there are exciting opportunities to further explore assemblage thinking. The concept offers useful nuance that provides actionable insights. There are now various ways of thinking with assemblages and this increasingly versatile toolkit provides a lens to study many of the various diffuse and globalised structures. This applies to a range of areas, although the concept has vast and largely untapped potential to study issues related to cyber security. As a nascent security issue, cyber security is still being defined and interpreted. Agreement on what components of cyber security should be public or private remain unsettled.

IR theory also has an established record of exploring the multiple and even clashing securities that can exist in a particular context – a central theme of this thesis. Indeed, one of the most significant implications of a diffuse security structure is the increased likelihood of fallout and disagreement over the form of cyber security being provided. This thesis is also shown that it is important to delve beyond the traditional units used in IR to explore that various visions of security that exist. While governments may differ from private sector firms, there is far more value in delving deeper – to examine what specific government departments want, to consider the incentives of individual private sector firms and account for the likely divergence that exists within such units.

While a core argument of this thesis has been that issues of security provision are underexplored, there is nonetheless much benefit to be derived from using assemblages to think about the offensive aspects of cyber campaigns. Offensive relationships between actors have regularly been presented through a proxy actor framework, yet this often neglects the agency of the so-called proxy and ignores the hybrid elements that exist between both parties. Whether

it be offensive Iranian cyber campaigns or Russian influence and disinformation operations, there are likely similar assemblage characteristics and structures at play. Here, there are likely interesting issues to explore related to the hybridity, harmony and distribution of power and incentive structures that exist within these assemblages. This thesis has shown how the assemblage processes discussed have fundamental implications for security provision, yet they almost certainly provide important insight for cyber offensive topics as well.

***

Beyond future research, the future of cyber security provision appears uncertain. This thesis has shown how assemblage dynamics and the balance of power shift rapidly. Roles and responsibilities are still being defined; the power and capabilities of a variety of security providers are growing and shrinking. All of the case studies examined are likely to look very different in ten years, yet there are broader and more substantial issues on cyber security provision that must be questioned and tracked. What role will governments eventually play in a cyber security capacity? Will traditional international organisations carve out a useful role and become meaningful cyber security players, or will other international networks supersede them? How will societies balance the economic interests of corporations with their broader role as security providers? It is these issues, which are fundamental to both cyber security studies and the future of IR, that make the issues addressed in this thesis fascinating to study.

This thesis has presented a variety of concepts and variables linked to assemblages, all of which have an influential bearing on cyber security provision. However, it is also important to look beyond simplistic narratives. Corporations are not just financially motivated while the security interests of government actors are not purely altruistic. Much of this has been acknowledged throughout this thesis, yet it is worth highlighting that there is substantial room for manoeuvre – space for all actors to change and shape future security dynamics. Notwithstanding certain

constraints, security providers remain capable of recognising a higher good and producing forms of security that are beneficial to society (rather than restricted to only their own narrow interests). Where disagreements occur, there is opportunities for these to occur in a healthy and productive manner, accounting for broader democratic principles. While such a reading might be considered over-optimistic, there is at least the possibility of developing more positive security assemblages.

A variety of factors determine the state of cyber security provision. Yet, this should not diminish or undermine the agency that any security provider has in working towards a more harmonious and shared notion of security that puts individuals at its core.

Bibliography

Primary Sources

Interviews

Clark, David (Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory). Interview by the author. Cambridge, MA. June 1, 2017.

Harvey, William (Senior Cyber Security Policy Advisor, Cabinet Office). Interview by the author. London. May 28, 2015.

Kutt, Andres (former Chief Advisor to RIA). Interview by the author. Skype. May 18, 2018.

Lellsaar, Mikk and Laura Kask (Ministry of Economic Affairs and Communications employees). Interview by the author and Lucas Kello. Tallinn, Estonia. April 26, 2017.

Segal, Adam (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). Interview by the author. Skype. March 20, 2018.

Cabinet Office employee. Interview by the author. Phone. June 20, 2015.

Chief Information Security Officer of a UK CNI Organisation. Interview by the author. London, UK. October 6, 2015.

Cyber security consultant (a) (working with UK Government clients). Interview by the author. London, UK. May 21, 2015.

Cyber security consultant (b) (working with UK Government clients). Interview by the author. London, UK. May 21, 2015.

Cyber security consultant (c) (working with UK and US Government clients). Interview by the author. London, UK. July 2, 2018.

Cyber security journalist. Interview by the author. London, UK. May 24, 2018.

Cyber security, privacy, and encryption academic. Interview by the author. Skype. April 11, 2018.

Department for Culture, Media and Sport employee. Interview by the author. London, UK. April 11, 2018.

Estonian Government employee. Interview by the author. Tallinn, Estonia. February 11, 2016.

Estonian Ministry of Defence employee. Interview by the author. Tallinn, Estonia June 18, 2015.

Former Government Communications Headquarters employee. Interview by the author. Oxford, UK. September 16, 2016.

Former National Security Agency lawyer. Interview by the author. Cambridge, Massachusetts. May 31, 2017.

International Centre for Defence and Security researcher. Interview by the author. Tallinn, Estonia. September 26 2016.

International Centre for Defence and Security researcher. Interview by the author. Skype. May 3, 2018.

National Cyber Security Centre employee. Interview by the author. London, UK. November 23, 2017.

Ministry of Economic Affairs and Communications Legal Advisor. Interview by the author. Skype. May 17, 2018.

NATO Cooperative Cyber Defence Centre of Excellence employee. Interview by the author. Tallinn, Estonia. June 24, 2015.

National Grid employee. Interview by the author. Warwick, UK. May 13, 2015.

Tallinn University of Technology researcher. Interview by the author. Skype. May 18, 2018.

Official Government and International Organisation Bills, Documents, Hearings, Reports, and Committee Evidence

Blaze, Matt. Testimony of Dr. Matt Blaze, § The Senate Committee on Commerce, Science, and Transportation, Subcommittee on Science, Technology and Space (1996). https://fas.org/irp/congress/1996_hr/960626_blaze_test.htm.

Blaze, Matt. Testimony of Dr. Matt Blaze, § US House of Representatives Committee on Government Oversight and Reform Information Technology Subcommittee Encryption Technology and Possible US Policy Responses (2015). http://www.crypto.com/papers/governmentreform-blaze2015.pdf.

Burr, Richard, and Diane Feinstein. Compliance with Court Orders Act of 2016 (2016). https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

Caproni, Valerie. "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security." Washington, D.C.." February 17, 2011

Collier, Jamie. "Written Evidence Submitted to the Joint Committee on Cyber Security: Critical National Infrastructure Inquiry." February 13, 2018. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/written/76828.pdf.

Comey, James. Senate Judiciary Committee (2015).

Grewe, Barbara A. "Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations." Washington, DC: Commission on Terrorist Attacks Upon the United States, August 20, 2004.

Joyce, Rob. "Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do," The White House, November 15, 2017, https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/.

Keeling, Chris. "Waking Shark II: Desktop Cyber Exercise Report to Participants." London, UK: British Banker's Association, November 12, 2013.

Lieu, Ted. To Preempt State Data Security Vulnerability Mandates and Decryption Requirements., Pub. L. No. 4528 (2016).

Rifkind, Sir Malcolm. "Intelligence and Security Committee: Annual Report 2011-2012." London, UK: Intelligence and Security Committee, July 5, 2012.

Rifkind, Sir Malcolm "Intelligence and Security Committee Foreign Involvement in the Critical National Infrastructure: the Implications for National Security Cm 8629." London, UK: Intelligence and Security Committee, June 3, 2013.

Rogers, Mike and Dutch Ruppersberger. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE." (Washington, DC: U.S. House of Representatives, October 8, 2012).

"2013 U.S. Intelligence Black Budget: Foreign Partner Access Project." United States Intelligence Community, 2013. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHe7fe.dir/doc.pdf.

"2014-2017 Cyber Security Strategy." Tallinn, Estonia: Ministry of Economic Affairs and Communications,2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

"A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation." Office of the Inspector General U.S. Department of Justice, March 2018.

"About CERT Estonia." Republic of Estonia Information System Authority, January 13, 2014. https://www.ria.ee/en/cert-estonia.html.

"About Us." CERT EU, accessed October 10, 2017. https://cert.europa.eu/cert/plainedition/en/cert_about.html.

"Administration System for the State Information System RIHA." Republic of Estonia Information System Authority, February 29, 2012. https://www.ria.ee/en/administration-system-of-the-state-information-system.html.

"Agenda Uruguay Digital 2020." Uruguay Digital, accessed April 18, 2018. https://www.agesic.gub.uy/innovaportal/file/125/3/agenda-uruguay-digital-2020---en.pdf.

"Aktors." e-Estonia, accessed April 30, 2018. https://e-estoniax.com/.

"Annual Cyber Security Assessment 2017." Tallinn, Estonia: Estonian Information System Authority, 2017. https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF.

"Britain's Cyber Security Bolstered by World-Class Strategy." GOV UK, November 1, 2016. https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.

"BULLRUN: PTF Lead for Special Operations and Policy." Government Communications Headquarters, accessed April 27, 2018. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0189/b2203e23.dir/doc.pdf.

"CESG," GOV UK, accessed February 2, 2016, https://www.gov.uk/government/organisations/cesg.

"Contracts Finder." GOV UK, accessed March 12, 2017. https://www.contractsfinder.service.gov.uk/Search/Results.

"Critical Information Infrastructure Protection CIIP." Republic of Estonia Information System Authority, June 10, 2017. https://www.ria.ee/en/ciip.html.

"Cyber Defence." NATO, February 17, 2017. http://www.nato.int/cps/en/natohq/topics_78170.htm.

"Cyber Europe." ENISA, April 26, 2017. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

"Cyber Exercises." ENISA, accessed October 11, 2017. https://www.enisa.europa.eu/topics/cyber-exercises.

"Cyber Insider." CPNI, accessed April 27, 2017. https://www.cpni.gov.uk/insider-threat.

"Cyber Security." Republic of Estonia Ministry of Economic Affairs and Communications, October 5, 2017. https://www.mkm.ee/en/objectives-activities/information-society/cyber-security.

"Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches," (Athens, Greece: ENISA, December 16, 2015).

"Cybersecurity and the Estonian Presidency." EU2017.EE, August 3, 2017. https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency.

"Cybersecurity Funding." The White House, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf.

"Data Exchange Layer X-Road." Estonian Information System Authority, accessed April 18, 2018, https://www.ria.ee/en/x-road.html.

"Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Office for Disarmament Affairs, accessed October 10, 2017. https://www.un.org/disarmament/topics/informationsecurity/.

"Documents." Republic of Estonia Information System Authority, April 13, 2016. https://www.ria.ee/en/documents.html.

"e-Identity." e-Estonia, accessed April 30, 2018. https://e-estonia.com/solutions/e-identity/id-card/.

"EU Cybersecurity Initiatives Working Towards a More Secure Online Environment." European Commission, January 2017. http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

"EU eGovernment Action Plan 2016-2020: Accelerating the Digital Transformation of Government." European Commissioner, April 19, 2016.

"Estonia Ready to Share Cyber Security Expertise with Iceland." Republic of Estonia Ministry of Foreign Affairs, June 20, 2017. http://vm.ee/en/news/estonia-ready-share-cyber-security-expertise-iceland.

"Estonian Defence Forces." Kaitsevägi, accessed April 25, 2018, http://www.mil.ee/en/defence-forces.

"Estonian Defence League's Cyber Unit." Kaitseliit, April 24, 2018. http://www.kaitseliit.ee/en/cyber-unit.

"Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation," *Obama Whitehouse Archive*, January 16, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

"Fact Sheet: Vulnerabilities Equities Process." Washington, DC: White House, November 15, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20White%20House%20Fact%20Sheet%20on%20VEP%20-%20FINAL%2011152017.PDF.

"Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." U.S.-Canada Power System Outage Task Force, April 2004.

"FIRST Teams." FIRST, accessed May 4, 2018. https://www.first.org/members/teams/.

"Forward Together: Our Plan for a Stronger Britain and a Prosperous Future," (The Conservative and Unionist Party Manifesto 2017, May 2017).

"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Sixty-Fifth Session." United Nations, July 30, 2010.

"Government Digital Strategy." London, UK: HM Government, November 2012. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf.

"Government Publishes Cyber Security Strategy." GOV UK, September 25, 2011. https://www.gov.uk/government/news/government-publishes-cyber-security-strategy.

"Government Transformation Strategy." GOV UK, February 9, 2017. https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy.

"Identity Documents." Politsei- ja Piirivalveamet, accessed April 30, 2018. https://www2.politsei.ee/en/teenused/isikut-toendavad-dokumendid/.

"Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government." Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, 2015. https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.

"Industry 100." NCSC, March 19, 2018. https://www.ncsc.gov.uk/information/industry-100-faq.

"Information System Authority." Republic of Estonia Information System Authority, October 14, 2016, https://www.ria.ee/en/about-estonian-information-system-authority.html.

"Inspectorate." Estonian Data Protection Inspectorate, November 22, 2017. http://www.aki.ee/en/inspectorate.

"Intelligence and Security Committee Annual Report 2010–2011." London, UK: HM Government, 2011.

"International Conferences." accessed October 18, 2017. https://www.enisa.europa.eu/topics/cyber-crisis-management/international-conference-series.

"Internet Freedom." U.S. Department of State, accessed March 29, 2018. https://www.state.gov/j/drl/internetfreedom/index.htm.

"Internet of Things and Industrial Control Systems." CPNI, accessed April 27, 2017. https://www.cpni.gov.uk/internet-things-and-industrial-control-systems.

"Interoperability of the State Information System." Tallinn, Estonia: Ministry of Economic Affairs and Communications, December 22, 2011.

"IT Infrastructure." Republic of Estonia Information System Authority, May 9, 2012. https://www.ria.ee/en/about-it-infrastructure.html.

"Mobile-ID." e-Estonia, accessed April 18, 2018. https://e-estonia.com/solutions/e-identity/id-card/.

"National-Level Cyber Crisis Management." ENISA, accessed October 11, 2017. https://www.enisa.europa.eu/topics/cyber-crisis-management/national-level-cyber-crisis-management?tab=details.

"National Cyber Security Strategy 2016-2021." London, UK: HM Government, November 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdfhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

"National Defence Strategy." Tallinn, Estonia: Estonian Ministry of Defence, 2011. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

"National Security Concept of Estonia." Ministry of Defence, 2017. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf;

"National Security Strategy and Strategic Defence and Security Review 2015." London, UK: HM Government, November 22, 2015.

"NCSC-Certified Degrees." NCSC, August 9, 2017. https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

"New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations." European Commissioner, 2017.

"New National Cyber Security Centre Becomes Operational," GCHQ, October 4, 2016. https://www.gchq.gov.uk/news-article/new-national-cyber-security-centre-becomes-operational.

"Office of Cyber Security and Information Assurance." GOV UK, accessed March 16, 2017. https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

"PRISM / US-984XN Overview, or The SIGAD Used Most in NSA Reporting Overview." National Security Agency: Special Source Operations, April 2013. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1979.dir/doc.pdf.

"Privacy Shield Overview," Privacy Shield, accessed April 1, 2018, https://www.privacyshield.gov/Program-Overview.

Raising Public Awareness about the Information Society." Republic of Estonia Information System Authority, December 28, 2015. https://www.ria.ee/en/programme.html.

"Read the Obama Administration's Draft Paper on Technical Options for the Encryption Debate." The Washington Post, accessed February 8, 2018. https://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/.

"Registered UK Organisations." Cyber Exchange, accessed October 25, 2017. https://cyberexchange.uk.net/#/directory.

"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." (United Nations, August 18, 2015).

"Security." Information Commissioner's Office, May 18, 2018. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

"Security and Safety." e-Estonia, accessed April 5, 2018. https://e-estonia.com/solutions/security-and-safety/.

"Snowden Surveillance Archive." Snowden Archive, accessed June 22, 2018. https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi.

"Special Source Operations: The Cryptographic Provider of Intelligence from Global High-Capacity Telecommunications Systems." National Security Agency, accessed April 27, 2018. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH5098.dir/doc.pdf.

"Supply Chain." CPNI, accessed April 27, 2017. https://www.cpni.gov.uk/supply-chain.

"Suur Arhitektuurinõukogu." Riigi Infosüsteemi Arhitektuur, September 14, 2016. https://www.ria.ee/riigiarhitektuur/wiki/doku.php?id=an:kohtumised:140916.

"Tallinn Declaration on EGovernment at the Ministerial Meeting During Estonian Presidency of the Council of the EU." EU2017, October 2017.

"Terrorism." Federal Bureau of Investigation, accessed July 17, 2018. https://www.fbi.gov/investigate/terrorism.

"The Digital Israel National Initiative: The National Digital Program of the Government of Israel." Ministry for Social Equality, June 2017. https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf.

"The Directive on Security of Network and Information Systems (NIS Directive)." European Commission, July 5, 2016. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

"The Estonian Informatics Centre Became the Estonian Information System's Authority." Republic of Estonia Information System Authority, June 16, 2011, https://www.ria.ee/en/the-estonian-informatics-centre-became-the-estonian-information-systems-authority.html.

"The Main Tasks of the EDL CU." Kaitseliit, accessed April 26, 2018. http://www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu.

"The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World." (London, UK: The Cabinet Office, November 2011). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Towards the next Defence and Security Review: Part One, 7th Report of Session 2013–14." (London, UK: House of Commons Defence Committee, December 18, 2013). https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/197/197.pdf.

"Trainings." ENISA, accessed October 11, 2017. https://www.enisa.europa.eu/topics/cyber-crisis-management/trainings.

"Transatlantic Exercise to Tackle Cyber Threat." GOV UK, November 12, 2015. https://www.gov.uk/government/news/transatlantic-exercise-to-tackle-cyber-threat.

"Transforming Digital Continuity." Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, May 2016.

"Trust Federation of Estonian X-Tee and Finnish Palvelyväylä: General Agreement Between Estonian Information System Authority and Finnish Population Register Centre." Estonian Information System Authority and Finnish Population Register Centre, September 29, 2016. https://esuomi.fi/wp-content/uploads/2016/09/RIA_VRK_Trust_federation_Agreement_.pdf;

"UK-India Defence and International Security Partnership." GOV UK, November 12, 2015. https://www.gov.uk/government/news/uk-india-defence-and-international-security-partnership.

"Vault 7: CIA Hacking Tools Revealed," WikiLeaks, March 7, 2017, https://wikileaks.org/ciav7p1/?

"Weeping Angel (Extending) Engineering Notes," WikiLeaks, accessed June 25, 2018, https://wikileaks.org/ciav7p1/cms/page_12353643.html.

"X-Road." e-Estonia, accessed April 30, 2018. https://e-estonia.com/solutions/interoperability-services/x-road/.

Statements and Speeches

Comey, James. "Expectations of Privacy: Balancing Liberty, Security, and Public Safety." Center for the Study of American Democracy Biennial Conference, Kenyon College Gambier, Ohio, April 6, 2016. https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety.

Comey, James. "The Complexities of Today's Security Challenges." presented at the Aspen Security Forum, London, UK, April 21, 2016. https://aspensecurityforum.org/global/.

Cook, Tim. "A Message to Our Customers." Apple, February 16, 2016. http://www.apple.com/customer-letter/.

Dorsey, Jack. Twitter post. February 18, 2016. https://twitter.com/jack/status/700457149227360256.

John Kerry and Urmas Paet, "Remarks at a Cyber Partnership Agreement Signing With Estonian Foreign Minister Urmas Paet" (Brussels, Belgium, December 3, 2013).

Lord Ahmad. "Foreign Office Minister condemns North Korean actor for WannaCry attacks." GOV UK, December 19, 2017. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

Obama, Barack. “Remarks by the President at South By Southwest Interactive.” Long Center for Performing Arts Austin, Texas, March 11, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive.

Osbourne, George. “Chancellor's Speech to GCHQ on Cyber Security.” GOV UK, November 17, 2015. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Maude, Francis. “UK Cyber Security Strategy: Statement on Progress 2 Years on.” GOV UK, December 12, 2013. https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-2-years-on.

Snowden, Edward. Twitter post. November 2, 2015. https://twitter.com/Snowden/status/661313394906161152.

Stoltenberg, General. “Press Conference by NATO Secretary General Jens Stoltenberg Following the North Atlantic Council Meeting at the Level of NATO Defence Ministers.” NATO, June 14, 2016, http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

Rosenstein, Rod J. “Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.” The United States Department of Justice, October 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

Vance, Jr, Cyrus R. Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, § United States Senate Committee on the Judiciary (2015). https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf.

Vance, Jr, Cyrus R. Cybersecurity and U.S. National Security, § United States Senate Committee on Armed Services (2016). https://www.armed-services.senate.gov/imo/media/doc/Vance_07-14-16.pdf.

“Vulnerabilities Equities Policy and Process for the United States Government.” Washington DC: The White House, November 15, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

Wray, Christopher. “Raising Our Game: Cyber Security in an Age of Digital Transformation.” presented at the FBI International Conference on Cyber Security, Fordham University, New York, January 9, 2018. https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

“Statement on Encryption.” Internet Association, November 23, 2015. https://internetassociation.org/112315encryption/.

Legal Acts and Documents

Burnstein v. United States Department of Justice, No. 97–16686 (United States Court of Appeals, Ninth Circuit. May 6, 1998).

Decker, Eileen M, Patricia A Donahue, Tracy L Wilkinson, and Allen W Chiu. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (United States District Court for the Central District of California February 16, 2016).

Orenstein, James. In Re Order Requiring Apple, INC. to Assist in the Execution of a Search Warrant Issued by this Court (United States District Court Eastern District of New York February 29, 2016).

Personal Data Protection Act 2008. https://www.riigiteataja.ee/en/eli/509072014018/consolide

Ramos, Michael A. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (United States District Court for the Central District of California March 3, 2016).

In re Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mJ-91, 2009 WL 424718 (United States District Court for the District of Vermont February 19, 2009).

Küberturvalisuse seadus 597 SE (2018). https://www.riigikogu.ee/tegevus/eelnoud/eelnou/.

Riigikogu. Emergency Act (2009). https://www.riigiteataja.ee/en/eli/525062014011/consolide.

Riigi Teataja. The Estonian Defence League Act (2013). https://www.riigiteataja.ee/en/eli/525112013006/consolide.

State of Emergency Act (1996). https://www.riigiteataja.ee/en/eli/530122013002/consolide.

United States of America v. Ramona Camelia Fricosu, a.k.a. Ramona Smith, No. 841 F.Supp.2d 1232 (United States District Court for the District of Colorado January 23, 2012).

United States of America v. Thomos J. Kirschner, No. 823 F. Supp. 2d 665 (United States District Court for the Eastern District of Michigan March 30, 2010).

The Constitution of the Republic of Estonia (1992) https://www.riigiteataja.ee/en/eli/521052015001/consolide.

Public Opinion Polls

Finkle, Jim. "Solid Support for Apple in iPhone Encryption Fight: Poll." Reuters, February 24, 2016. https://www.reuters.com/article/us-apple-encryption-poll/solid-support-for-apple-in-iphone-encryption-fight-poll-idUSKCN0VX159.

Smith, Matthew. "Nationalisation vs Privatisation: the Public View." YouGov, May 19, 2017. https://yougov.co.uk/news/2017/05/19/nationalisation-vs-privatisation-public-view/.

"Reuters/Ipsos Poll: Apple vs the FBI." Reuters, February 23, 2016. http://fingfx.thomsonreuters.com/gfx/rngs/1/883/1284/APPLE-ENCRYPTION-POLL.jpg.

"More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone." Washington, DC; Pew Research Center, February 22, 2016. http://assets.pewresearch.org/wp-content/uploads/sites/5/2016/02/2-22-2016-iPhone-release.pdf.

Secondary Sources

Academic Publications

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Journal of Cybersecurity* 1, no. 1 (November 17, 2015): 69–79.

Abrahamsen, Rita, and Michael C. Williams. "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3, no. 1 (March 2009): 1–17.

Abrahamsen, Rita, and Michael C Williams. *Security Beyond the State: Private Security in International Politics*. Cambridge, UK: Cambridge University Press, 2011.

Abrahamsen, Rita, and Michael C Williams. "Tracing Global Assemblages, Bringing Bourdieu to the Field: A Conversation with Rita Abrahamsen and Michael Williams." In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 25–31. London, UK: Palgrave Macmillan UK, 2014.

Acuto, Michele, and Simon Curtis, eds. *Reassembling International Theory*. London, UK: Palgrave Macmillan UK, 2014.

Acuto, Michele, and Simon Curtis. "Assemblage Thinking and International Relations." In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 1–15. London, UK: Palgrave Macmillan UK, 2014.

Adler, Emanuel, and Vincent Pouliot. “International Practices.” *International Theory* 3, no. 1 (2011): 1–36.

Adler, Emanuel, and Vincent Pouliot. *International Practices*. Cambridge, UK: Cambridge University Press, 2011.

Adler-Nissen, Rebecca, ed. *Bourdieu in International Relations*. Abingdon, UK: Routledge, 2013.

Adler-Nissen, Rebecca. “Towards a Practice Turn in EU Studies: The Everyday of European Integration.” *Journal of Common Market Studies* 54, no. 1 (November 2015): 87–103.

Aldrich, Richard J. *GCHQ*. London, UK: Harper Press, 2010.

Aldrich, Richard J and Christopher R Moran. “‘Delayed Disclosure’: National Security, Whistle-Blowers and the Nature of Secrecy.” *Political Studies* (March 28, 2018).

Alon, Ilan, Hua Wang, Jun Shen, and Wenxian Zhang. “Chinese State-Owned Enterprises Go Global.” *Journal of Business Strategy* 35, no. 6 (2014): 3–18.

Anderson, Robert H and Anthony C Hearn, “An Exploration of Cyberspace Security R&D Investment Strategies for DARPA ‘the Day After...in Cyberspace II.’” (RAND, 1996).

Areng, Liina. “Lilliputian States in Digital Affairs and Cyber Security.” *The Tallinn Papers*, no. 4 (2014).

Baldwin, David A. “Power and International Relations.” In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse, and Beth A Simmons, 273-297. London, UK: Sage, 2007.

Balzacq, Thierry and Myriam Dunn Cavelty. “A Theory of Actor-Network for Cyber-Security.” *European Journal of International Security*, May 12, 2016, 1–23.

Bamford, James. *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America*. New York: Anchor, 2009.

Beamer, Glenn. “Elite Interviews and State Politics Research.” State Politics & Policy Quarterly 2, no.1 (2002): 86-96.

Bennett, Andrew and Colin Elman. “Case Study Methods in the International Relations Subfield.” *Comparative Political Studies* 40, no. 2 (June 30, 2007): 170-195.

Berndtsson, Joakim and Maria Stern. “Private Security and the Public-Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage.” *International Political Sociology* 5, no. 4 (December 5, 2011).

Betz, David and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower*. Abingdon, UK: Routledge, 2011.

Biernacki, Patrick and Dan Waldorf. “Snowball Sampling: Problems and Techniques of Chain Referral Sampling.” *Methods and Research* 10, no.2 (November 1981): 141-163.

Bigo, Didier. “Globalized (in)Security: the Field and the Ban-Opticon.” in *Illiberal Practices of Liberal Regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala 10-48. Abingdon, UK: Routledge, 2008.

Bousquet, Antoine. “Welcome to the Machine: Rethinking Technology and Society through Assemblage Theory.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 91–97. London, UK: Palgrave Macmillan UK, 2014.

Brummer, Alex. *Britain for Sale: British Companies in Foreign Hands – the Hidden Threat to Our Economy*. New York: Random House, 2012.

Budiansky, Stephen. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union*. New York: Alfred A. Knoff, 2016.

Bueger, Christian. “Thinking Assemblages Methodologically: Some Rules of Thumb.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 58–66. London, UK: Palgrave Macmillan UK, 2014.

Bureš, Oldřich. *Private Security Companies*: Transforming Politics and Security in the Czech Republic. London, UK: Palgrave Macmillan, 2015.

Buzan, Barry. *People, States & Fear*. Colchester, UK: ECPR Press, 2016.

Buzan, Barry and Richard Little. “Waltz and World History: the Paradox of Parsimony.” *International Relations* 23, no. 3 (October 7, 2009): 446.

Buzan, Barry, Ole Wæver, and Jaap de Wilder. *Security: A New Framework of Analysis*. Boulder, CO: Lynne Rienner, 1998.

Cabrera, Yvette, Rory Carroll, and Tom Dart. “San Bernardino Shooting Victim ‘Had Argued with Killer About Islam.’” The Guardian, December 5, 2015. http://www.theguardian.com/us-news/2015/dec/05/san-bernardino-victim-had-argued-with-shooter-about-islam.

Caldwell, Tracey. “Call the Digital Fire Brigade.” *Network Security* 2014, no. 3 (March 14, 2014): 5–8.

Cardash, Sharon L., Frank J. Cilluffo, and Rain Ottis. “Estonia’s Cyber Defence League: A Model for the United States?” *Studies in Conflict & Terrorism* 36, no. 9 (September 2013): 777–87.

Cardenas, Alvaro A, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and Shankar Sastry. “Challenges for Securing Cyber Physical Systems.” *Workshop on Future Directions in Cyber-Physical Systems Security*, 2009.

Carr, Madeline. “Power Plays in Global Internet Governance.” *Millennium: Journal of International Studies* 43, no. 2 (January 2015): 640–59.

Carr, Madeline. “Public-Private Partnerships in National Cyber-Security Strategies.” *International Affairs* 92, no. 1 (January 2016): 43–62.

Carr, Madeline. *US Power and the Internet in International Relations*. London, UK: Palgrave Macmillan, 2016.

Cavelty, Myriam Dunn and Manuel Suter. “Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection.” *International Journal of Critical Infrastructure Protection* 2, no. 4 (December 2009): 179–187.

Cavelty, Myriam Dunn. “The Militarisation of Cyber Security as a Source of Global Tension.” Edited by Daniel Möckli and Andreas Wenger. *Strategic Trends Analysis*, February 1, 2012.

Cavelty, Myriam Dunn. “The Militarisation of Cyberspace: Why Less May Be Better.” In *2012 4th International Conference on Cyber Conflict*, 141–53. Tallinn, Estonia, 2012.

Cavelty, Myriam Dunn. “Cyber-Security and Private Actors.” In *Routledge Handbook of Private Security Studies*, edited by Rita Abrahamsen and Anna Leande, 65–71. Abingdon, UK: Routledge, 2015.

Chamorro-Premuzic, Tomas, and Nathalie Nahai. “Why We’re So Hypocritical About Online Privacy.” Harvard Business Review, May 1, 2017. https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, UK: Verso, 2014.

Collier, Jamie. “Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom.” In *Ethics and Policies for Cyber Operations*, 187–212. Philosophical Studies Series. Cham, Switzerland: Springer, 2017.

Collier, Jamie. “Proxy Actors in the Cyber Domain: Implications for State Strategy.” *St Antony’s International Review* 13, no. 1 (2017): 25–47.

Collier, Jamie. “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision.” *Politics and Governance* 6, no. 2 (June 11, 2018): 13–21.

Collier, Jamie and Jantje Silomon. “Security Dichotomies in Cyber Security.” (British International Studies Association 41st Annual International Conference 2016, Edinburgh, UK, June 15-17, 2016).

Collier, Jamie and Andrew Martin. “Beyond Awareness: the Breadth and Depth of the Cyber Skills Needed” *Cyber Studies Working Paper* (forthcoming).

Collier, Stephen J. “Assemblages and the Conduct of Inquiry: a Conversation with Stephen J. Collier.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 32-38. London, UK: Palgrave Macmillan UK, 2014.

Coole, Diana and Samantha Frost, eds. *New Materialisms: Ontology, Agency and Politics* (Durham, UK: Duke University Press, 2010).

Corry, Olaf. “Global Assemblages and Structural Models of International Relations.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 48-56. London, UK: Palgrave Macmillan, 2013.

Cox, Robert W. “Social Forces, States and World Orders: Beyond International Relations Theory.” *Millennium* 10, no. 2 (June 1981): 126-155.

Curtis, Simon. *The Power of Cities in International Relations*. New York: Routledge, 2014

Curtis, Simon. “Cities and Global Governance: State Failure or a New Global Order?” *Millennium* 44, no. 3 (May 25, 2016): 455–77.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. “Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.” NATO CCDCOE, 2011.

Dahl, Robert A. “The Concept of Power,” *Behavioural Science* 2, no. 3 (July 1957): 201–15.

Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Toronto, Canada: Signal, 2013.

Deibert, Ronald J. “Circuits of Power: Security in the Internet Environment.” In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, edited by James N. Rosenau and JP Singh, 115-142. Albany, GA: State University of New York Press, 2002.

Deibert, Ronald J. “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace.” *Millennium* 32, no. 3 (December 2003): 501–30.

DeLanda, Manuel. *Intensive Science and Virtual Philosophy*. London, UK: Continuum, 2002.

DeLanda, Manuel. *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London, UK: Continuum, 2006.

DeLanda, Manuel. *Deleuze: History and Science*. New York: Atropos, 2010.

Deleuze, Giles and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*. London, UK: University of Minnesota Press, 1987.

Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." *IEEE transactions on Information Theory* 22, no. 6 (November 1976): 644-654.

Dourado, Eli. “Working Paper: Is There a Cyber Security Market Failure?” *Mercatus Center Working Paper* 12, no. 5 (January 23, 2012): 1–34.

Eckstein, Harry. “Case Study and Theory in Political Science.” In *Case Study Method*, edited by Roger Gomm, Martyn Hammersley, and Peter Foster, 119-164. London, UK: SAGE Publications, 2000.

Edwards, Chris. “Margaret Thatcher’s Privatization Legacy.” *CATO Journal* 37, no. 1 (February 1, 2017): 89–101.

Erskine, Toni and Madeline Carr. “Beyond ‘Quasi-Norms’: the Challenges and Potential of Engaging with Norms in Cyberspace.” In *International Cyber Norms Legal, Policy Industry Perspectives*, edited by Anna-Maria Osula and Henry Rõigas, 87–109. Tallinn, Estonia: NATO CCDCOE, 2016.

Egloff, Florian. “Cybersecurity and the Age of Privateering: A Historical Analogy.” *Cyber Studies Working Paper Series* 1 (2015).

Egloff, Florian. “State, Semi-State, and Non-State Actors in Cybersecurity.” (Understanding Change in World Politics nternational Studies Association 58th Annual Convention, Baltimore, MA, February 22-25, 2017).

Egloff, Florian. “Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates.” Oxford, UK: University of Oxford, 2018.

Farrell, Henry and Martha Finnemore. “The End of Hypocrisy: American Foreign Policy in the Age of Leaks.” *Foreign Affairs* 92, no. 6 (November 2013): 22–26.

Fierke, Karin M. *Critical Approaches to International Security*. Cambridge, UK: Polity Press, 2015.

Flyverbom, Mikkel. “Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations.” In *Power, Policy and Profit: Corporate Engagement in Politics and Governance*, edited by Christina Garsten and Adrienne Sörbom 115-133. Cheltenham, UK: Edward Elgar Publishing, 2017.

Gallie, Walter B. “Essentially Contested Concepts.” *Proceedings of the Aristotelian Society* 56, (1956): 167–98.

Geertz, Clifford. *The Interpretation of Cultures*. New York, Basic Books 1973.

Germano, Judith H. “Cybersecurity Partnerships: A New Era of Public-Private Collaboration.” (The Center on Law and Security, NYU School of Law, October 2014). http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.

Giles, Keir and Kim Hartmann. “Cyber Defense: An International View.” Fort Belvoir, VA: Strategic Studies Institute and U.S. Army War College Press, September 1, 2015.

Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press, 2018.

Gold, Steve. “The SCADA Challenge: Securing Critical Infrastructure.” *Network Security* 2009, no. 8 (August 1, 2009): 18–20.

Gomm, Roger, Martyn Hammersley, and Peter Foster, eds. *Case Study Method*. London, UK: SAGE Publications, 2000.

Graham, Robert. “How Terrorists Use Encryption.” *CTC Sentinel* 9, no. 6 (June 2016): 20–25.

Grigsby, Alex. “The End of Cyber Norms.” *Survival* 59, no. 6 (November 2017): 109–22.

Haggerty, Kevin D and Richard V Ericson, “The Surveillant Assemblage.” *British Journal of Sociology* 51, no. 4 (December, 2003): 605–22.

Hansen, Lene, and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53, no. 4 (December 2009): 1155–75.

Harrop, Wayne and Ashley Matteson. “Cyber Resilience: a Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA.” *Journal of Business Continuity Emergency Planning* 7, no. 1 (March 7, 2014): 149–62.

Harvey, William S. “Strategies for Conducting Elite Interviews.” *Qualitative Research* 11, no. 4 (2011): 431-441. pp. 436.

Hayden, Michael. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

Hinsley, Sir Harry. “The Influence of ULTRA in the Second World War.” presented at the Security Group Seminar, Babbage Lecture Theatre, University of Cambridge Computer Laboratory, Cambridge, UK, October 19, 1993.

Hollis, Martin and Steve Smith, *Explaining and Understanding in International Relations*. Oxford, UK: Oxford University Press, 1991.

Hurel, Louise Marie and Luisa Cruz Lobato. “Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs.” *Journal of Cyber Policy* (April 27, 2018): 61-76.

Jackson, Patrick Thaddeus. *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics*. Abingdon, UK: Routledge, 2011.

Jackson, Camille Marie. “Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success.” *New Voices in Public Policy* 7 (2013).

Jagasia, Arnav. “A Look into Public Private Partnerships for Cybersecurity.” Public Policy Initiative, University of Pennsylvania, April 18, 2017. https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

Jordan, Paul. “Nation Branding: A Tool for Nationalism?” *Journal of Baltic Studies* 45, no. 3 (2013): 283–303.

Kangas, Anni. “Global Cities, International Relations and the Fabrication of the World.” *Global Society* 31, no. 4 (June 2017): 531–50.

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38, no. 2 (October 2013): 7–40.

Kello, Lucas. “Data Embassies: Consequences for National Security and State Survival.” Unpublished manuscript, 2016.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.

King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994.

Kitsing, Meelis. “Success Without Strategy: E-Government Development in Estonia.” *Policy & Internet* 3, no. 1 (January 1, 2011): 1–21.

Klingova, Katarina. “Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia.” Department of Political Science, Central European University, 2013.

Knake, Rob. “Obama's Cyberdoctrine: Digital Security and the Private Sector.” *Foreign Affairs*, May 6, 2016. https://www.foreignaffairs.com/print/1117450.

Krause, Keith and Michael C Williams, “Broadening the Agenda of Security Studies: Politics and Methods,” *Mershon International Studies Review* 40, no. 2 (1996): 229-254.

Kvochko, Elena and Rajiv Pant.“Why Data Breaches Don’t Hurt Stock Prices.” *Harvard Business Review*, March 31, 2015. https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

Laar, Mart. “The Estonian Economic Miracle.” *Backgrounder* 2060 (August 2007): 1–12.

Lawson, Nigel. “Economy: The New Conservatism.” presented at the Lecture to the Bow Group, London, UK, August 4, 1980. https://www.margaretthatcher.org/document/109505.

Lazarus, Jeffrey, Amy McKay and Lindsey Herbel, “Who Walks Through the Revolving Door? Examining the Lobbying Activity of Former Members of Congress.” *Interest Groups & Advocacy* 5, no. 1 (January 2016): 82-100.

Leech, Beth L. *Lobbyists at Work*. New York: Apress, 2013.

Lippert, Randy and Daniel O'Connor, “Security Assemblages: Airport Security, Flexible Work, and Liberal Governance,” *Alternatives* 28, no. 3 (2003): 351–58.

Lisle, Debbie. “Energising the International.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 67-74. London, UK: Palgrave Macmillan, 2013.

Lundborg, Tom and Nick Vaughan-Williams. “New Materialisms, Discourse Analysis, and International Relations: A Radical Intertextual Approach.” *Review of International Studies* 41, no. 1 (2015): 3–25.

Lynn III, William J. “Defending a New Domain: The Pentagon’s Cyberstrategy.” *Foreign Affairs* 89, no. 5 (September 2010): 97–108.

Mac Ginty, Roger. “A Material Turn in International Relations: The 4x4, Intervention and Resistance.” *Review of International Studies* 43, no. 5 (December 2017): 855-874.

Mahoney, James. “After KKV: The New Methodology of Qualitative Research.” *World Politics* 62, no. 1 (2010): 120–47.

Margetts, Helen and Andre Naumann, “Government as a Platform: What Can Estonia Show the World?” *Cyber Studies Research Paper* (February 28, 2017).

Martin, Keith M. *Everyday Cryptography: Fundamental Principles and Applications*. New York: Oxford University Press, 2012.

Martinovic, Ivan, Lucas Kello, and Ivo Sluganovic. “Blockchains for Governmental Services: Design Principles, Applications, and Case Studies.” *Cyber Studies Working Paper*, no. 7 (November 2017).

Matthews, Ron and Nellie Zhang Yan. “Small Country ‘Total Defence’: A Case Study of Singapore.” *Defence Studies* 7, no. 3 (September 2007): 376–95.

Maurer, Tim. “Cyber Proxies and the Crisis in Ukraine.” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 79–86. Tallinn, Estonia: NATO CCDCOE, 2015.

McFate, Sean. *The Modern Mercenary: Private Armies and What They Mean for World Order*. New York: Oxford University Press, 2014.

Meinrath, Sascha D and Sean Vitka. “Crypto War II.” *Critical Studies in Media Communication* 31, no. 2 (March 15, 2014): 123–28.

Merton, Robert K, Majorie Fiske, and Patricia L Kendall. *The Focused Interview: A Manual of Problems and Procedures*. (New York: Free Press, 1990).

Moore, Daniel and Thomas Rid. “Cryptopolitik and the Darknet.” *Survival* 58, no. 1 (January, 2016): 7–38.

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. New York: Alfred A Knopf, 1963.

Morriss, Peter. *Power: A Philosophical Analysis*. Manchester, UK: Manchester University Press, 2002.

Muller, Lilly. “How to Govern Cyber Security? The Limits of the Multi-Stakeholder Approach and the Need to Rethink Public-Private Cooperation.” In *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, edited by Karsten Friis and Jens Ringsmose 116–29. Abingdon, UK: Routledge, 2016.

Mumford, Andrew. *Proxy Warfare*. Cambridge, UK: Polity Press, 2013.

Mumford, Andrew. “Proxy Warfare and the Future of Conflict.” *The RUSI Journal* 158, no. 2 (April 2013): 40–46.

Musa, Shavana. “Data Protection, Intelligence-Sharing and Brexit: The Path Ahead,” August 2, 2017.

Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. “SCADA Security in the Light of Cyber-Warfare.” *Computers & Security* 31, no. 4 (June 1, 2012): 418-436.

Nye Jr, Joseph S. *The Future of Power*. New York: Public Affairs, 2011.

Oakley, Aimee. “New Labour and the Continuation of Thatcherite Policy.” *POLIS Journal* 6 (2011): 1–37.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*. London, UK: William Heinemann, 2013.

Ong, Aihwa and Stephen J Collier. *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*. Oxford, UK: Blackwell, 2005.

Anna-Maria Osula, “National Cyber Security Organisation: Estonia.” Tallinn, Estonia: NATO CCDCOE, 2015.

Osula, Anna-Maria. “National Cyber Security Organisation: United Kingdom.” Tallinn, Estonia: NATO CCDCOE, 2015.

Ottis, Rain. “From Pitchforks to Laptops Volunteers in Cyber Conflicts.” Tallin, Estonia: NATO CCDCOE, 2010. https://ccdcoe.org/publications/2010proceedings/Ottis%20-%20From%20Pitchforks%20to%20Laptops%20Volunteers%20in%20Cyber%20Conflicts.pdf.

Owens, Patricia. “Distinctions, Distinctions: ‘Public’ and ‘Private” Force?’” *International Affairs* 84, no. 5 (September 1, 2008): 977–90.

Paalman, Matijn. “The Copenhagen School in the Fifth Domain: Successfully Securitizing Cyberspace?” Department of Peace and Conflict Research, Uppsala University, 2013.

Priisalu, Jaan and Rain Ottis. “Personal Control of Privacy and Data: Estonian Experience.” *Health and Technology* 7, no. 4 (December 2017): 441–451.

Rattray, Gregory J and Jason Healey. “Non-State Actors and Cyber Conflict.” In *Americas Cyber Future Security and Prosperity in the Information Age*, edited by Kristin M Lord and Travis Sharp, 65–86. Washington, DC: Center for a New American Security, 2011).

Rid, Thomas. *Cyber War Will Not Take Place*. London, UK: Hurst, 2013.
Rothstein, Robert L. *Alliances and Small Powers*. New York: Columbia University Press, 1968.

Sassen, Saskia. *Territory, Authority, Rights: From Medieval to Global Assemblages*. Woodstock, UK: Princeton University Press, 2006.

Sassen, Saskia, and Aihwa Ong. “The Carpenter and the Bricoleur: A Conversation with Saskia Sassen and Aihwa Ong.” In *Reassembling International Theory*, edited by Michele Acuto and Simon Curtis, 17–24. London, UK: Palgrave Macmillan UK, 2014.

Schatzki, Theodore R, Karin Knorr Cetina, and Eike von Savigny, eds. *The Practice Turn in Contemporary Theory*. London, UK: Routledge, 2005.

Schmidt, Andreas. “The Estonian Cyberattacks.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey. Vienna, VA: Cyber Conflict Association, 2013.

Schmitt, Michael N and Liis Vihul, “Proxy Wars in Cyberspace: the Evolving International Law of Attribution,” *Fletcher Security Review* 1, no. 2 (June 26, 2014): 53–72.

Seawright, Jason and John Gerring, “Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options.” *Political Research Quarterly* 61, no. 2 (2008): 294–308.

Singer, Peter W. *Corporate Warriors: The Rise of the Privatized Military Industry*. Ithaca, NY: Cornell University Press, 2008.

Singer, Peter W and Allan Friedman, *Cybersecurity and Cyberwar*. New York : Oxford University Press, 2014.

Song, Hyojin, and Simon Wilkie. “The Price of Privacy in the Cloud: The Economic Consequences of Mr. Snowden,” February 2017. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf.

Stein, George J. “Total Defense: A Comparative Overview of the Security Policies of Switzerland and Austria.” *Defence Analysis* 6, no. 1 (1990): 17-33.

Soghoian, Christopher. “Snowden’s Leaks Have Finally Forced Companies to Enhance Their Security.” MIT Technology Review, December 17, 2013. https://www.technologyreview.com/s/522756/snowdens-leaks-have-finally-forced-companies-to-enhance-their-security/.

Stake, Robert E. “Qualitative Case Studies.” In *Strategies of Qualitative Inquiry*, edited by Norman K Denzin and Yvonna S Lincoln, 119-150. Thousand Oaks, CA, SAGE Publications, 2008.

Stoddart, Kristan. “UK Cyber Security and Critical National Infrastructure Protection.” *International Affairs* 92, no. 5 (August 29, 2016): 1079-1105.

Tammpuu, Piia and Anu Masso, “‘Welcome to the Virtual State’: Estonian e-Residency and the Digitalised State as a Commodity.” *European Journal of Cultural Studies* (January 29, 2018).

Tilly, Charles. *Coercion, Capital and European States AD 990–1990*. Oxford, UK: Basil Blackwell, 1990.

Valeriano, Brandon and Ryan C Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.

Verba, Sidney. “Some Dilemmas in Comparative Research.” *World Politics* 20, no. 1 (October 1967): 111-127.

Voelkner, Nadine. “Tracing Human Security Assemblages.” In *Research Methods in Critical Security Studies*, edited by Mark B Salter and Can E Mutlu, 203-206. Abingdon, UK: Routledge, 2013.

Waltz, Kenneth N. “Reflections on Theory of International Politics: A Response to My Critics.” In *Neorealism and Its Critics*, edited by Robert O Keohane, 322–45 . New York: Columbia University Press, 1986

Warren, Mark E. “Max Weber’s Nietzchean Conception of Power.” *History of the Human Sciences* 5, no. 3 (1992): 19–37.

Weber, Max. *An Outline of Interpretive Sociology*. Edited by Guenther Roth and Claus Wittich. Berkeley, CA: University of California Press, 1978.

Weber, Max. “Politics as a Vocation.” In *From Max Weber: Essays in Sociology*, edited by Hans Heinrich Gerth and Charles Wright Mills, 77–128. Abingdon, UK: Routledge, 2009.

Willis, Ben. “The Advantages and Limitations of Single Case Study Analysis.” *E-International Relations*, July 5, 2014. http://www.e-ir.info/2014/07/05/the-advantages-and-limitations-of-single-case-study-analysis/.

Yin, Robert K. *Case Study Research: Design and Methods*, 4th ed. (Thousand Oaks, CA: SAGE, 2009).

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.

Industry and think-tank reports and documents

Ablon, Lillian, Martin C Libicki, and Andrea A Golay. "Markets for Cybercrime Tools and Stolen Data; Hackers' Bazaar." RAND, March 2014.

Acton, Brian. "Signal Foundation." Signal, February 21, 2018. https://signal.org/blog/signal-foundation/.

Albright, David, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Washington, DC: Institute for Science and International Security, December 22, 2010.

Barker, Elaine B. "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms." Gaithersburg, MD: National Institute of Standards and Technology, August 2016.

"Data Security." Internet Association, accessed April 1, 2018. https://internetassociation.org/positions/data-security/.

"Diplomatic Immunity for Data: Estonia Creates a Virtual Embassy." Microsoft, December 14, 2017. https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/.

"Exercise Locked Shields 2016 Highlights Priorities in Cyber Defence." (Tallinn, Estonia: NATO CCDCOE, April 21, 2016).

Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32 Stuxnet Dossier." Symantec, February 2011. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Gillmor, Daniel Kahn and Jay Stanley. "A Few Easy Steps Everyone Should Take to Protect Their Digital Privacy." ACLU, June 7, 2016. https://www.aclu.org/blog/privacy-technology/internet-privacy/few-easy-steps-everyone-should-take-protect-their-digital.

Heller, Charles E. "Economy of Force: A Total Army, the Israel Defense Force Model." Strategic Studies Institute and U.S. Army War College, March 1, 1992.

Kaska, Kadri, Anna-Maria Osula, and LTC Jan Stinissen. "The Cyber Defence Unit of the Estonian Defence League." Tallinn, Estonia: NATO CCDCOE, 2013.

Kehl, Danielle, Andi Wilson, and Kevin Bankston. "Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s." Washington, DC: Open Technology Institute, New America, June 2015.

Lund, Joshua. "Signal Partners with Microsoft to Bring End-To-End Encryption to Skype." Signal, January 11, 2018. https://signal.org/blog/skype-partnership/.

Madden, Mary. "Public Perceptions of Privacy and Security in the Post-Snowden Era." Washington, DC: Pew Research Center, November 12, 2014).

Pettitt, Matthew. "Encryption at Rest: Not the Panacea to Data Protection." Manchester, UK: NCC Group Whitepaper, 2017.

Olmstead, Kenneth and Aaron Smith, "Americans and Cyber Security." (Washington, DC: Pew Research Center, January 2017). http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Opsahl, Kurt."Facebook's Eroding Privacy Policy: A Timeline." Electronic Frontier Foundation, April 28, 2010, https://www.eff.org/deeplinks/2010/04/facebook-timeline.

Pernik, Piret. “National Cyber Security Strategies The Estonian Approach.” International Centre for Defence Studies, June 22, 2017. https://www.cncs.gov.pt/content/files/estonian_cyber_security_strategy_-_piret_pernik.pdf.

Pernik, Piret and Emmet Tuohy. “Cyber Space in Estonia: Greater Security, Greater Challenges.” International Centre for Defence Studies, August 2013.

Schulz, Wolfgang and Joris van Hoboken. “Human Rights and Encryption.” Paris, France: UNESCO, 2016. http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.

Shlapak, David and Michael Johnson. “Reinforcing Deterrence on NATO’s Eastern Flank: Wargaming the Defense of the Baltics.” RAND Corporation, 2016.

Smith, Brad. “The Need for a Digital Geneva Convention,” Microsoft on the Issues, February 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Toms, Mike. “The Thatcher Privatisation Legacy: Not Quite What She Planned?” (London, UK: Oxera Agenda, May 2013).

“About National Grid.” National Grid, accessed October 5, 2017. http://www2.nationalgrid.com/About-us/.

“About Us.” Scottish Water, accessed October 5, 2017. http://www.scottishwater.co.uk/about-us.

“About Us.” United Utilities, accessed October 5, 2017. https://www.unitedutilities.com/help-and-support/about-us/

“About Us.” Yorkshire Water, accessed October 5, 2017. https://www.yorkshirewater.com/about-us.

“Agreed Sale of Affinity Water,” (Morgan Stanley and Infracapital, May 2, 2017). https://www.infracapital.co.uk/Controls/Brochure/-/media/Infracapital/PDFs/Press%20Releases/Infracapital-agrees-sale-of-Affinity-Water.pdf.

“Apple Differential Privacy Technical Overview,” Apple. https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.

“Data Security.” Internet Association, accessed April 1, 2018. https://internetassociation.org/positions/data-security/.

“Encryption Policy in Democratic Regimes Finding Convergent Paths and Balanced Solutions.” New York: EastWest Institute, 2018. https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf?dm_i=439P,3E9,1AF62,7Z5,1

“Facebook: A Privacy Guide.” ACLU, accessed April 1, 2018. https://www.aclu.org/other/facebook-privacy-guide.

“FIRST Vision and Mission Statement.” FIRST, accessed October 10, 2017. https://www.first.org/about/mission.

“Government Data Collection.” Internet Association, accessed April 1, 2018. https://internetassociation.org/positions/law-enforcement/.

“iOS Security.” (Cupertino, CA: Apple, September, 2014).

“iOS Security.” (Cupertino, CA: Apple, March 16, 2017).

“IOS Security: IOS 11.” (Cupertino, CA: Apple, January 2018).

“Mitigating Security Risk in the National Infrastructure Supply Chain.” London, UK: CPNI, June 2017.

“News Releases 2016.” Atkins, October 20, 2016. http://www.atkinsglobal.com/en-gb/media-centre/news-

releases/2016/oct/2016-10-20uk.

“Our Company.” Portsmouth Water, accessed October 5, 2017. https://www.portsmouthwater.co.uk/about-us/.

“Our Members.” Internet Association, accessed April 1, 2018. https://internetassociation.org/our-members/.

“Pricing.” ProtonMail, accessed March 28, 2018. https://protonmail.com.

“Privacy.” Internet Association, accessed April 1, 2018. https://internetassociation.org/positions/privacy/.

“Promoting a Secure Internet.” New America, accessed April 1, 2018. https://www.newamerica.org/oti/promoting-secure-internet/.

“Secure Messaging Scorecard.” Electronic Frontier Foundation, November 3, 2014. https://www.eff.org/node/82654.

“Statement on Encryption.” Internet Association, November 23, 2015. https://internetassociation.org/112315encryption/.

“We Are the Voice of the Internet Economy.” Internet Association, accessed April 1, 2018. https://internetassociation.org/.

“Shareholder Centre.” National Grid, accessed October 5, 2017. http://investors.nationalgrid.com/shareholder-centre.aspx.

“Read This Before You Rail Against Encryption.” New America, accessed April 1, 2018. /weekly/101/read-this-before-you-rail-against-encryption/.

“Telegram F.A.Q.” Telegram, accessed March 28, 2018. https://telegram.org/faq.

“TRISIS Malware Analysis of Safety System Targeted Malware.” Hanover, MD: Dragos, December 14, 2017.

“UN GGE.” Geneva Internet Platform Digital Watch, accessed October 10, 2017. https://dig.watch/processes/ungge.

“X-ROAD: A Secure Data Exchange Layer for Building e-Governments.” Tallinn, Estonia: Cybernetica, 2014. https://cyber.ee/uploads/2013/06/X-ROAD_technical_whitepaper_2014.pdf.

“Youlgrave Waterworks Ltd: a Brief History,” Youlgrave Waterworks, accessed October 3, 2017, http://www.youlgrave.org.uk/?page_id=51.

Patents

Zeidler, Howard M. End-to-End Encryption System and Method of Operation. 4,578,530. SanMateo, CA, issued March 25, 1986. https://patentimages.storage.googleapis.com/a7/3b/16/eb638400c54c83/US4578530.pdf.

Film and Videos

Poitras, Laura. *Citizenfour*. Praxis Films, 2014.

Rasmus Merivoo. *Anna Piperal - Ambassador of E-Estonia*. Accessed April 27, 2018. https://www.youtube.com/watch?time_continue=75&v=bvEQrn9oVaU.

infosysteemiamet. *X-Road Introduction (Long Version)*, 2016. https://www.youtube.com/watch?v=9PaHinkJlvA.

News and websites

Aitel, Dave and Matt Tait, “Everything You Know About the Vulnerability Equities Process Is Wrong,” Lawfare, August 18, 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

Alba, Davey. “Google and Facebook Still Reign Over Digital Advertising.” Wired, July 29, 2017. https://www.wired.com/story/google-facebook-online-ad-kings/.

Anderton, Kevin. “Privacy Versus Security; How Americans View the Issue of Encryption.” Forbes, February 16, 2017. https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/kevinanderton/2017/02/16/privacy-versus-security-how-americans-view-the-issue-of-encryption-infographic/.

Ashford, Warwick. “Is UK Critical National Infrastructure Properly Protected?” *Computer Weekly*, March 3, 2011. http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.

Ashford, Warwick. “UK Government Sets Up Cyber Security Fusion Cell.” Computer Weekly, March 27, 2013. https://www.computerweekly.com/news/2240180207/UK-government-sets-up-cyber-security-fusion-cell.

Asthana, Anushka and Heather Stewart. “Labour Party's Plan to Nationalise Mail, Rail and Energy Firms.” The Guardian, May 11, 2017. https://www.theguardian.com/politics/2017/may/10/labour-party-manifesto-pledges-to-end-tuition-fees-and-nationalise-railways.

Ball, James, Julian Borger, and Glenn Greenwald. “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security.” The Guardian, September 6, 2013. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Barrett, Brian. “The Year Encryption Won.” Wired, December 23, 2016, https://www.wired.com/2016/12/year-encryption-won/.

Barzilay, Omri. “3 Ways Blockchain Is Revolutionizing Cybersecurity.” Forbes, August 21, 2017. https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/.

Basu, Eric. “Target CEO Fired - Can You Be Fired if Your Company Is Hacked?” Forbes, June 15, 2014. https://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/#1dea5f7e7c9f.

Bauter, Alison. “FBI vs. Apple: Massachusetts Judge Sided with Feds in Gang Case, Records Show.” Boston Patch, April 8, 2016. https://patch.com/massachusetts/boston/judge-sides-fbi-against-apple-boston-gang-case-0.

Benner, Katie and Joseph Goldstein. “Apple Wins Ruling in New York iPhone Hacking Order.” The New York Times, February 29, 2016. https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.htm.

Berger, Joseph. “A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case.” The New York Times, March 25, 2016. https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

Biddle, Sam and Micah Lee. “The CIA Didn’t Break Signal or WhatsApp, Despite What You’ve Heard,” *The Intercept*, March 7, 2017. https://theintercept.com/2017/03/07/the-cia-didnt-break-signal-or-whatsapp-despite-what-youve-heard/.

Bing, Chris. “Why Is State Department Silent in the Global Encryption Debate?” *Fedscoop*, June 24, 2016. https://www.fedscoop.com/should-the-state-department-be-more-involved-in-the-encryption-debate/.

Bing, Chris. “Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms.” Cyberscoop, May 24, 2018. https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/.

Blitz, James and Daniel Thomas, “Parliamentary Report Raises Alarm Over Lack of Checks on Huawei.” Financial Times, June 6, 2013. https://www.ft.com/content/d3680d06-cecb-11e2-8e16-00144feab7de.

Brandom, Russell. “Why the NSA Is Staying Out of Apple's Fight with the FBI.” *The Verge*, March 9, 2016. http://www.theverge.com/2016/3/9/11186868/apple-fbi-nsa-encryption-exploit-hack.

Brandom, Russel. “With its Retreat in New York, the FBI has Lost the Encryption Fight.” The Verge, April 25, 2016. https://www.theverge.com/2016/4/25/11501992/fbi-apple-new-york-case-unlock-iphone-lost.

Brodkin, Jon. “FBI Security Expert: Apple Are ‘Jerks’ About Unlocking Encrypted Phones.” Ars Technica, January 11, 2018. https://arstechnica.com/tech-policy/2018/01/fbi-security-expert-apple-are-jerks-about-unlocking-encrypted-phones/.

Burgess, Matt. “Everything You Need to Know About EternalBlue – the NSA Exploit Linked to Petya.” Wired, June 28, 2017. http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

Carman, Ashley. “An Israeli Company Is Reportedly Helping the FBI Crack the San Bernardino iPhone.” The Verge, March 23, 2016. https://www.theverge.com/2016/3/23/11290374/apple-iphone-fbi-encryption-crack-cellebrite.

Cadwalladr, Carole and Emma Graham-Harrison. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” The Guardian, March 17, 2018. http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Chambers, Joshua. “Why Estonia Hasn’t Built a Government Digital Service.” GovInsider, May 10, 2016. https://govinsider.asia/digital-gov/why-estonia-hasnt-built-a-government-digital-service/.

Clark, Pilita. “GCHQ Intervenes to Secure Smart Meters Against Hackers.” Financial Times, March 18, 2016. https://next.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8.

Cobb, Stephen. “Is the World Ready for GDPR? Privacy and Cybersecurity Impacts Are Far-Reaching.” We Live Security, May 23, 2017. https://www.welivesecurity.com/2017/05/23/gdpr-is-world-ready-cybersecurity-impact/.

Cohen, Tova. “Israeli Firm Helping FBI to Open Encrypted iPhone: Report.” Reuters, March 23, 2016. http://www.reuters.com/article/us-apple-encryption-cellebrite-idUSKCN0WP17J.

Collier, Jamie. “Getting Intelligence Agencies to Adapt to Life Out of the Shadows.” *Council on Foreign Relations*, April 5, 2017. https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows.

Conger, Kate. “Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program.” Gizmodo, June 1, 2018. https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620.

Copeland, Jack. “Alan Turing: The Codebreaker Who Saved ’Millions of Lives.” BBC News, June 19, 2012, http://www.bbc.co.uk/news/technology-18419691.

Cox, Joseph. “GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS.” *Motherboard,* April 29, 2016. http://motherboard.vice.com/read/gchq-vulnerabilities-mozilla-apple.

Cox, Joseph. “Encryption Gets in The Way of 75% of Cases, Europol Chief Says.” Motherboard, May 10, 2016, https://motherboard.vice.com/en_us/article/4xa3jq/encryption-gets-in-the-way-of-75-of-cases-europol-chief-rob-wainwright.

Cox, Joseph. “Military, FBI, and ICE Are Customers of Controversial ‘Stalkerware.’” Motherboard, February 23, 2018. https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware.

Cox, Joseph. “Government Malware Company ‘Grey Heron’ Advertises Signal, Telegram Spyware.” Motherboard, March 7, 2018. https://motherboard.vice.com/en_us/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team.

Cox, Joseph. “Documents Prove Local Cops Have Bought Cheap iPhone Cracking Tech.” Motherboard, March 9, 2018. https://motherboard.vice.com/en_us/article/xw5bqz/documents-prove-local-cops-have-bought-cheap-iphone-cracking-tech.

Cox Joseph and Lorenzo Franceschi-Bicchierai. “How a Tiny Startup Became the Most Important Hacking Shop You’ve Never Heard Of.” Motherboard, February 7, 2018. https://motherboard.vice.com/en_us/article/8xdayg/iphone-zero-days-inside-azimuth-security.

Crouse, Megan. “Tech Companies Lobby for Security, National Trade.” ECN, April 28, 2015. https://www.ecnmag.com/article/2015/04/tech-companies-lobby-security-national-trade.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” Wired, August 21, 2007. https://www.wired.com/2007/08/ff-estonia/.

de Looper, Christian. “Apple Is Preparing To Make iMessage App Even Safer,” Digital Trends, June 9, 2017, https://www.digitaltrends.com/mobile/apple-ios-11-imessage-security/

Dewey, Caitlin. “98 Personal Data Points That Facebook Uses to Target Ads to You.” The Washington Post, August 19, 2016. https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/.

Duckett, Chris. “Australia Will Lead Five Eyes Discussions to ‘Thwart’ Terrorist Encryption: Brandis,” ZD Net, June 26, 2017. http://www.zdnet.com/article/australia-will-lead-five-eyes-discussions-to-thwart-terrorist-encryption-brandis/.

Farivar, Cyrus. “Massachusetts High Court Orders Suspect to Decrypt His Computers.” Ars Technica, June 26, 2014. https://arstechnica.com/tech-policy/2014/06/massachusetts-high-court-orders-suspect-to-decrypt-his-computers/.

Farivar, Cyrus. “Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot.” Ars Technica, September 18, 2014, https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

Fedorov, Ava. “Simulation Exercise Tests UK Response to Cyber-Terrorism.” SC Magazine, January 27, 2015. https://www.scmagazineuk.com/simulation-exercise-tests-uk-response-cyber-terrorism/article/1478940.

Fiegerman, Seth. “Obama’s Staff Is Taking over Silicon Valley.” CNN Money, August 11, 2016. http://money.cnn.com/2016/08/11/technology/obama-staff-silicon-valley/index.html.

Fiveash, Kelly. “GCHQ Losing Its ‘Internet Whizzes’ to Microsoft, Google.” The Register, July 14, 2011. https://www.theregister.co.uk/2011/07/14/gchq_microsoft_google/.

Fox-Brewster, Thomas. “The Feds Can Now (Probably) Unlock Every iPhone Model In Existence – UPDATED.” Forbes, February 26, 2018. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#6dc73b17667a.

Gardham, Duncan. ‘Whizz Kids Deserting the Spy World as Threat of Attacks Increases.’ The Telegraph, July 13, 2011. http://www.telegraph.co.uk/news/uknews/terrorism-in-the- uk/8635959/Whizz-kids-deserting-the-spy-world-as-threat-of-attacks-increases.html.

Geller, Eric. “Congress Plans Encryption Investigations as Paris Attacks Reignite ‘Crypto Wars.’” The Daily Dot, November 18, 2015. https://www.dailydot.com/layer8/encryption-backdoors-congress-investigations-surveillance-paris-attacks/.

Geller, Eric. “White House Ducks Petition’s Demand for Strong Encryption.” The Daily Dot, December 9, 2015. https://www.dailydot.com/layer8/white-house-encryption-backdoors-petition-response/.

Geller, Eric. “Heads of 2 Powerful House Committees Join Anti-Encryption Crusade.” The Daily Dot, December 11, 2015. https://www.dailydot.com/layer8/encryption-backdoors-terrorism-surveillance-congress-house-chairmen/.

Geller, Eric. “California Lawmaker Introduces Human-Trafficking Bill That Bans Strong Encryption.” The Daily Dot, January 21, 2016. https://www.dailydot.com/layer8/california-encryption-backdoors-legislation-human-trafficking/.

Geller, Eric. “Senate Homeland Security Chairman: Encryption Law Could ‘Do More Harm Than Good.’” The Daily Dot, January 28, 2016. https://www.dailydot.com/layer8/encryption-ron-johnson-backdoors-crypto-wars-aei-event/.

Geller, Eric. “‘Crypto Wars’ Timeline: A History of the New Encryption Debate.” The Daily Dot, April 26, 2016. https://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/.

Gellman, Barton and Laura Poitras. “U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program.” The Washington Post, June 7, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gellman, Barton and Ashkan Soltani. “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.” The Washington Post, October 30, 2013. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.f22c4898ed97.

Gibbs, Samuel. “San Bernardino iPhone Hack Won’t Work on Newer Models, Says FBI.” The Guardian, April 7, 2016. http://www.theguardian.com/technology/2016/apr/07/san-bernardino-iphone-hack-work-newer-models-fbi-james-comey.

Green, Mathew. “Is Apple Picking a Fight With the U.S. Government?” Slate, September 23, 2014.http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html.

Greenburg, Andy. “Meet ‘Project Zero,’ Google’s Secret Team of Bug-Hunting Hackers.” Wired, July 15, 2014. https://www.wired.com/2014/07/google-project-zero/.

Greenberg, Andy. “The Senate’s Draft Encryption Bill Is ‘Ludicrous, Dangerous, Technically Illiterate.’” Wired, April 8, 2016. https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/.

Greenberg, Andy. “You Can Finally Encrypt Facebook Messenger, So Do It.” Wired, October 4, 2016. https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/.

Greenwald, Glenn. “NSA Collecting Phone Records of Millions of Verizon Customers Daily.” The Guardian, June 6, 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. “Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations.” The Guardian, June 11, 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Grigsby, Alex and Adam Segal. “Silicon Valley and Washington Can Be Friends If They Take These Steps.” Fortune, February 2, 2017. http://fortune.com/2017/02/02/silicon-valley-washington-relationship-tech-donald-trump-encryption/.

Gunaratna, Shanika. “The Snowden Effect: Silicon Valley vs. the Government.” CBS News, June 6, 2016. https://www.cbsnews.com/news/the-snowden-leaks-effect-its-now-silicon-valley-vs-the-government-privacy/.

Hachman, Mark. “The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers.” PC World, October 1, 2015. https://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html.

Hall, Kat. “Cybersecurity Is Slowing Down My Business, Say Majority of Chief Execs.” The Register, February 17, 2016. https://www.theregister.co.uk/2016/02/17/cyber_security/.

Hall, Kat. “Security Execs Must Prep for Post-Brexit Cyber Challenges.” The Register, June 11, 2018. https://www.theregister.co.uk/2018/06/11/cisos_must_be_braced_for_cyber_security_challenges_post_brexit_report/.

Hammersley, Ben. “Concerned about Brexit? Why Not Become an e-Resident of Estonia.” Wired UK, March 27, 2017. http://www.wired.co.uk/article/estonia-e-resident.

Hankewitz, Sten. “Estonia and Japan to Sign a Cyber Security Cooperation Treaty.” Estonian World, December 18, 2017. http://estonianworld.com/security/estonia-japan-sign-cyber-security-cooperation-treaty/.

Herlihy, Peter. “Government as a Data Model': What I Learned in Estonia.” Government Digital Services, October 31, 2013. https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.

Hill, Henry. “The Wit and Wisdom of Nick Timothy. Stop Selling Our Security to China.” Conservative Home, July 15, 2016. http://www.conservativehome.com/parliament/2016/07/the-wit-and-wisdom-of-nick-timothy-19-stop-selling-our-security-to-china.html.

Hille, Kathrin, Stephanie Kirchgaessner, and Paul Taylor. “China and the US: Access Denied.” Financial Times, April 7, 2011. https://www.ft.com/content/9080ccaa-614d-11e0-ab25-00144feab49a.

Hopkins, Nick and Julian Borger. “Exclusive: NSA Pays £100m in Secret Funding for GCHQ.” The Guardian, August 1, 2013. https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

Hosenball, Mark. “FBI Paid under $1 Million to Unlock San Bernardino iPhone.” Reuters, May 4, 2016. https://uk.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUKKCN0XQ032.

Hudson, John. “Citing Paris Attack, CIA Director Criticizes Surveillance Reform Efforts.” Foreign Policy, November 16, 2015. https://foreignpolicy.com/2015/11/16/citing-paris-attack-cia-director-criticizes-surveillance-reform-efforts/.

Hurn, Alex. “Apple Calls on UK Government to Scale Back Snooper's Charter.” *The Guardian*, May 21, 2015. https://www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill.

Ingram, David. “Hearing Scheduled in Apple Encryption Case for March 22.” Reuters, February 19, 2016. https://www.reuters.com/article/apple-encryption-hearing/hearing-scheduled-in-apple-encryption-case-for-march-22-u-s-justice-dept-idUSL2N15Y1RF.

Jones, Sam. “GCHQ Chief to Say Free Market Failing on Cyber Security.” Financial Times, November 9, 2015. https://next.ft.com/content/4ec3e438-8708-11e5-90de-f44762bf9896.

Sam Jones and George Parker. “GCHQ Seeks to Allay Hinkley Security Fears.” Financial Times, October 16, 2015. https://www.ft.com/content/d3fc0cb6-740c-11e5-a129-3fcc4f641d98.

Kang, Cecilia and Juliet Eilperin. “Why Silicon Valley Is the New Revolving Door for Obama Staffers.” The Washington Post, February 28, 2015. https://www.washingtonpost.com/business/economy/as-obama-nears-close-of-his-tenure-commitment-to-silicon-valley-is-clear/2015/02/27/3bee8088-bc8e-11e4-bdfa-b8e8f594e6ee_story.html

Karsten, Jack. “Alternative Perspectives on Encryption.” Brookings, May 12, 2016. https://www.brookings.edu/blog/techtank/2016/05/12/alternative-perspectives-on-encryption/.

Kerry, Cameron F. “The Backdoor Threat to Encryption.” The Boston Globe, October 1, 2015. https://www.bostonglobe.com/opinion/editorials/2015/10/01/the-backdoor-threat-encryption/xprHAyG12AAFCVvrrkE6OO/story.html.

Korzak, Elaine. “The 2015 GGE Report: What Next for Norms in Cyberspace?” Lawfare, September 23, 2015. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

Korzak, Elaine. “UN GGE on Cybersecurity: The End of an Era?” The Diplomat, July 31, 2017. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Krebs, Brian. “Paris Terror Attacks Stoke Encryption Debate.” Krebs on Security, November 17, 2015. https://krebsonsecurity.com/2015/11/paris-terror-attacks-stoke-encryption-debate.

Krebs, Brian. “Computer Virus Cripples UK Hospital System.” Krebs on Security, November 2, 2016. https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/.

Kuchler, Hannah. “Tech Companies Step Up Encryption in Wake of Snowden.” Financial Times, November 4, 2014. https://www.ft.com/content/3c1553a6-6429-11e4-bac8-00144feabdc0.

Kuchler, Hannah. “Why Obama’s West Wingers Went West.” Financial Times, January 10, 2018. https://www.ft.com/content/56712806-f58f-11e7-88f7-5465a6ce1a00.

Landler, Mark and John Markoff. “Digital Fears Emerge After Data Siege in Estonia.” The New York Times, May 29, 2007. https://www.nytimes.com/2007/05/29/technology/29estonia.html.

Lawson, Ewan. “The Joint Forces Command and the 2015 SDSR: Too Soon to Tell?” RUSI, November 27, 2015. https://rusi.org/commentary/joint-forces-command-and-2015-sdsr-too-soon-tell.

Lecher, Colin. “Government Withdraws from New York iPhone Unlocking Case.” The Verge, April 22, 2016. https://www.theverge.com/2016/4/22/11492804/fbi-apple-new-york-iphone-unlocking-case-withdrawl.

Lee, Micah. “Encrypting Your Laptop Like you Mean It.” The Intercept, April 27, 2015. https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/.

Levy, Stephen. “Battle of the Clipper Chip.” The New York Times, June 12, 1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

Leyden, John. “UK Joins US Financial Institutions for Industry Resilience Tests.” The Register, November 19, 2015. https://www.theregister.co.uk/2015/11/19/resilient_shield/.

Lucas, Edward. “Against Putin, It’s Time to Channel JFK.” POLITICO Magazine, August 22, 2014. http://www.politico.com/magazine/story/2014/08/only-obama-can-stop-putin-now-110264.html.

Luckerson, Victor. “How the ‘John Oliver Effect’ Is Having a Real-Life Impact.” *Time*, July 10, 2015. http://time.com/3674807/john-oliver-net-neutrality-civil-forfeiture-miss-america/.

Lynch, Jennifer. “Newly Released Documents Detail FBI’s Plan to Expand Federal Surveillance Laws.” Electronic Frontier Foundation, February 16, 2011. https://www.eff.org/deeplinks/2011/02/newly-released-documents-detail-fbi-s-plan-expand.

Lynch, Sarah N and Brendan Pierson. “U.S. Attorney General Says Tech Companies Should Help Access Encrypted Evidence.” Reuters, November 2, 2017. https://www.reuters.com/article/us-usa-justice-encryption/u-s-attorney-general-says-tech-companies-should-help-access-encrypted-evidence-idUSKBN1D21V2.

Macalister, Terry. “Hinkley Point C: No Easy Solution to Theresa May's Chinese Puzzle.” The Guardian, September 3, 2016. https://www.theguardian.com/uk-news/2016/sep/03/hinkley-point-c-theresa-may-china-g20-summit.

Mansel, Tim. “How Estonia Became E-Stonia,” *BBC News*, May 16, 2013. http://www.bbc.co.uk/news/business-22317297.

Martin, James. “Encrypted Messaging Apps.” CNET, March 23, 2016. https://www.cnet.com/uk/pictures/timeline-a-history-of-encryption-and-government-backdoors-pictures/9/.

McCormick, Rich. “Donald Trump Is Using an iPhone Now.” The Verge, March 29, 2017. https://www.theverge.com/2017/3/29/15103504/donald-trump-iphone-using-switched-android.

McCrum, Dan. “City’s Embrace of China Comes with Risks.” Financial Times, October 22, 2015. https://www.ft.com/content/6b9fd03e-78d1-11e5-933d-efcdc3c11c89?mhq5j=e5

McCullagh, Declan. “FBI: We Need Wiretap-Ready Web Sites - Now.” CNET, May 4, 2012. https://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” BBC News, April 27, 2017. https://www.bbc.co.uk/news/39655415.

McLannahan, Ben, David J Lynch, and Chloe Cornish. “Equifax Shares Drop as Questions Mount Over Data Breach.” Financial Times, September 8, 2017. https://www.ft.com/content/f503ef3c-94b2-11e7-a9e6-11d2f0ebb7f0?mhq5j=e5.

McLaughlin, Jenna. “New Court Filing Reveals Apple Faces 12 Other Requests to Break Into Locked iPhones.” The Intercept, February 23, 2016. https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

McLaughlin, Jenna. “NSA Is Mysteriously Absent From FBI-Apple Fight.” The Intercept, March 3, 2016. https://theintercept.com/2016/03/03/nsa-is-mysteriously-absent-from-fbi-apple-fight/.

McLaughlin, Jenna. “NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says.” *The Intercept*, June 10, 2016. https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/.

Medeiros, João. “WannaCry Laid Bare the NHS‘ Outdated IT Network – and it’s Still Causing Problems.” Wired, May 24, 2017. http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware.

Menn, Joseph, and Dustin Volz. “Apple Case Exposes Ongoing Government Rift over Encryption Policy.” Reuters, March 8, 2016. https://www.reuters.com/article/us-apple-encryption-schism-insight/apple-case-exposes-ongoing-government-rift-over-encryption-policy-idUSKCN0W70U5.

Meeks, Brock N. “Clipping Clipper: Matt Blaze.” Wired, September 1, 1994. https://www.wired.com/1994/09/clipping-clipper-matt-blaze/.

Miller, Claire Cain. “Revelations of N.S.A. Spying Cost U.S. Tech Companies.” The New York Times, March 21, 2014. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

Moody, Glyn. “Paris Terrorists Used Burner Phones, Not Encryption, to Evade Detection.” Ars Technica, March 21, 2016. https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/.

Morbin, Tony. “Nuclear Weapons Vulnerable to Cyber-Attack Due to Outdated Legacy Systems.” SC Magazine, January 22, 2018. https://www.scmagazineuk.com/nuclear-weapons-vulnerable-cyber-attack-due-outdated-legacy-systems/article/1473487.

Nakashima, Ellen. “Why the Sony Hack Drew an Unprecedented U.S. Response against North Korea.” *The Washington Post*, January 15, 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html.

Natalucci, Matteo. “Canada and Uruguay Join Digital 5 Government Group.” Government Computing Network, February 22, 2018. http://central-government.governmentcomputing.com/news/canada-and-uruguay-join-digital-5-government-group-6063639.

Naughton, John. “Google, Not GCHQ, Is the Truly Chilling Spy Network.” The Guardian, June 18, 2017. https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network.

O’Neill, Patrick Howell. “Android 7 Boasts New Encryption Features as the Crypto War Soldiers On.” The Daily Dot, August 24, 2016. https://www.dailydot.com/layer8/android-nougat-encryption/.

O’Neill, Patrick Howell. “Sen. Dianne Feinstein Wants to Bring Back Bill That Bans Strong Encryption.” *Cyberscoop*, November 10, 2017. https://www.cyberscoop.com/dianne-feinstein-encryption-bill-fbi-apple/.

Oberhaus, Daniel. “How the Government Is Waging Crypto War 2.0.” Motherboard, August 10, 2016, https://motherboard.vice.com/en_us/article/jpgvy3/encryption-debate-the-end-of-end-to-end

Ong, Thuy. “The FBI inflated the number of encrypted phones linked to crime.” The Verge, May 23, 2018. https://www.theverge.com/2018/5/23/17383496/fbi-encrypted-phones-inflated-number-crime.

Paletta, Damian. “How the U.S. Fights Encryption–and Also Helps Develop It.” The Wall Street Journal, February 22, 2016. https://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096.

Parker, George and Christopher Adams. “UK Paves Path for West’s First China-Designed Nuclear Reactor.” Financial Times, September 21, 2015. https://www.ft.com/content/52462048-5f8b-11e5-a28b-50226830d644?mhq5j=e5.

Parker, George and Elaine Moore. “George Osborne Says UK and China ‘Will Stick Together.’” Financial Times, September 22, 2015. https://www.ft.com/content/be5c0e8c-607b-11e5-9846-de406ccb37f2.

Perez, Evan and Shimon Prokupecz. “Paris Attackers Likely Used Encrypted Apps, Officials Say.” CNN, December 17, 2015. https://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/index.html.

Perlroth, Nicole and Clifford Krauss. “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.” The New York Times, March 16, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

Perloth, Nicole, Jeff Larson, and Scott Shane. “N.S.A. Able to Foil Basic Safeguards of Privacy on Web.” The New York Times, September 5, 2013. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2.

Peterson, Andrea and Ellen Nakashima, “Obama Administration Explored Ways to Bypass Smartphone Encryption,” The Washington Post, September 24, 2015. https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html.

Phillips, Tom. “Edward Snowden: Hong Kong Hotel Hideaway of the NSA Whistleblower.” The Telegraph, June 10, 2013. https://www.telegraph.co.uk/news/worldnews/asia/hongkong/10110927/Edward-Snowden-Hong-Kong-hotel-hideaway-of-the-NSA-whistleblower.html.

Pilkington, Ed. “Guardian and Washington Post Win Pulitzer Prize for NSA Revelations.” The Guardian, April, 14, 2014, https://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations.

Rajab, Talal. “Briefing with James Snook on National Cyber Security Strategy.” techUK, June 21, 2016. https://www.techuk.org/insights/meeting-notes/item/8704-briefing-with-james-snook-on-national-cyber-security-strategy.

Reed, John. “Unit 8200: Israel's Cyber Spy Agency.” Financial Times, July 12, 2015. https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c.

Reeve, Tom. “Industry's Cyber-Security “Market Failure” Must Be Addressed.” SC Magazine, May 23, 2016, http://www.scmagazineuk.com/industrys-cyber-security-market-failure-must-be-addressed/article/498249/.

Reitman, Rainey. “Partial Victory: Obama Encryption Policy Rejects Laws Mandating Backdoors, But Leaves the Door Open for Informal Deals.” Electronic Frontier Foundation, October 9, 2015. https://www.eff.org/deeplinks/2015/10/partial-victory-obama-encryption-policy-reject-laws-mandating-backdoors-leaves.

Rid, Thomas. “How Russia Pulled Off the Biggest Election Hack in U.S. History.” Esquire, October 20, 2016, https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/.

Rid, Thomas. “Why Twitter Is the Best Social Media Platform for Disinformation.” November 1, 2017. https://motherboard.vice.com/en_us/article/bj7vam/why-twitter-is-the-best-social-media-platform-for-disinformation.

Roberts, Jeff John. “Here Are the Most Popular Apps for Secure Messages.” Fortune, January 17, 2017. http://fortune.com/2017/01/17/most-popular-secure-apps/.

Rosenzweig, Paul. “The United Kingdom and Huawei.” Lawfare, July 25, 2013. https://www.lawfareblog.com/united-kingdom-and-huawei.

Rubin, Joel, James Queally, and Paresh Dave. “FBI Unlocks San Bernardino Shooter’s iPhone and Ends Legal Battle With Apple, For Now.” Los Angeles Times, March 28, 2016. http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

Sanger, David E and Brian X. Chen. “Signalling Post-Snowden Era, New iPhone Locks Out N.S.A.” The New York Times, September 26, 2014. https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

Schneier, Bruce. “FBI/CIA/NSA Information Sharing Before 9/11,” Schneier on Security, November 11 2009. https://www.schneier.com/blog/archives/2009/11/fbiciansa_infor.html.

Schneier, Bruce. “Schneier on Security,” Schneier on Security, accessed March 26, 2018, https://www.schneier.com/.

Schneier, Bruce. “A ‘Key’ for Encryption, Even for Good Reasons, Weakens Security.” The New York Times, July 15, 2016. https://www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security.

Schneier, Bruce. “Who Are the Shadow Brokers?” *The Atlantic*, May 23, 2017. https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Selyukh, Alina. “The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?” NPR, February 23, 2016. https://www.npr.org/sections/alltechconsidered/2016/03/23/470573608/the-apple-fbi-whodunit-whos-helping-the-feds-crack-the-locked-iphone.

Sevastopulo, Demetri. “Huawei Pulls Back the Curtain on Ownership Details.” Financial Times, February 27, 2014. https://www.ft.com/content/469bde20-9eaf-11e3-8663-00144feab7de.

Shoorbajee, Zaid. “Playing Nice? FireEye CEO Says U.S. Malware Is More Restrained than Adversaries.” Cyberscoop, June 1, 2018. https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice/.

Simon, Emma. “Thatcher's Legacy: How Has Privatisation Fared?” The Telegraph, April 12, 2013. http://www.telegraph.co.uk/finance/personalfinance/investing/shares-and-stock-tips/9989430/Thatchers-legacy-how-has-privatisation-fared.html.

Smeets, Max and James Shires, “Cyber Exceptionalism.” New America, December 7, 2017, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/cyber-exceptionalism/.

Stern-Peltz, Mikkel and Jim Armitage. “IT Firms Lose Billions After NSA Scandal Exposed by Whistleblower Edward Snowden.” The Independent, December 29, 2013. https://www.independent.co.uk/life-style/gadgets-and-tech/news/it-firms-lose-billions-after-nsa-scandal-exposed-by-whistleblower-edward-snowden-9028599.html.

Solon, Olivia and Sabrina Siddiqui. “Forget Wall Street – Silicon Valley Is the New Political Power in Washington.” *The Guardian*, March 11, 2017. https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington.

Sorcher, Sara. “The Battle between Washington and Silicon Valley over Encryption.” CS Monitor. http://projects.csmonitor.com/cryptowars.

Sottek, T C, and Janus Kopfstein. “Everything You Need to Know About PRISM.” The Verge, July 17, 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Spring, Tom. “Apple Tackles Cellebrite Unlock Claims, Sort Of,” Threatpost, February 27, 2018. https://threatpost.com/apple-tackles-cellebrite-unlock-claims-sort-of/130111/.

Stewart, Heather. “UK and US to Simulate Cyber-Attack on Nuclear Plants to Test Resilience.” The Guardian, March 30, 2016. https://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience.

Sullivan, Mark. “Why The FBI Chose To Try The Apple Encryption Case In The Media.” Fast Company, February 22, 2016. https://www.fastcompany.com/3057033/why-the-fbi-chose-to-try-the-apple-encryption-case-in-the-media.

Swinford, Steven and Emily Gosden. “Theresa May Delays Hinkley Nuclear Decision Amid Concerns Over Chinese Involvement.” The Telegraph, July 29, 2016. http://www.telegraph.co.uk/business/2016/07/29/theresa-may-delays-hinkley-nuclear-decision-amid-concerns-over-c/.

Swinhoe, Dan. “Why More and More Companies Are Turning to Bug Bounties.” IDG Connect, April 30, 2018. https://www.idgconnect.com/abstract/30307/why-companies-bug-bounties.

Tambur, Silver. “The Estonian President Invites Everyone to Become an E-Resident.” Estonian World, December 1, 2016. http://estonianworld.com/business/estonian-president-invites-everyone-become-e-resident/.

Tambur, Silver. “Estonia to Move Ahead With the ‘Data Embassy’ Concept.” Estonian World, March 22, 2018. http://estonianworld.com/security/estonia-move-ahead-data-embassy-concept/.

TheShadowBrokers. “REPOST: TheShadowBrokers Message#1 - August 2016.” Steemit, June 30, 2017. https://steemit.com/shadowbrokers/@theshadowbrokers/repost-theshadowbrokers-message-1-august-2016.

Thielman, Sam and Spencer Ackerman, “Cozy Bear and Fancy Bear: Did Russians Hack Democratic Party and if So, Why?” *The Guardian*, June 29, 2016. https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc.

Thomas, Daniel. “Huawei Does Not Pose Risk to UK National Security, Report Finds.” Financial Times, March 25, 2015. https://www.ft.com/content/70592668-d2e4-11e4-a792-00144feab7de.

Thomson, Iain. “Cops Hate Encryption but the NSA Loves It When You Use PGP.” The Register, January 27, 2016. https://www.theregister.co.uk/2016/01/27/nsa_loves_it_when_you_use_pgp/.

Thomson, Iain. “Everything You Need to Know About the Petya, Er, NotPetya Nasty Trashing PCs Worldwide.” The Register, June 28, 2017. https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

Timberg, Craig. “Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police.” The Washington Post, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.291bfbbb3650

Timm, Trevor. “Four Ways Edward Snowden Changed the World – and Why the Fight’s Not Over.” The Guardian, June 5, 2014. http://www.theguardian.com/commentisfree/2014/jun/05/what-snowden-revealed-changed-nsa-reform.

Timm, Trevor. “Paris Is Being Used to Justify Agendas That Had Nothing to Do with the Attack.” The Guardian, November 20, 2015. https://www.theguardian.com/commentisfree/2015/nov/20/paris-attacks-political-agenda-immigration-encryption-surveillence.

Turnham, Steve. “NSA Chief Says Trump Has Not Directed Him to Counter Russian Meddling.” ABC News, February 27, 2018. http://abcnews.go.com/Politics/nsa-chief-trump-directed-counter-russian-meddling/story?id=53393061.

Turton, William. “WhatsApp Rolls out End-to-End Encryption to All 1 Billion Users.” The Daily Dot, April 5, 2016, https://www.dailydot.com/layer8/whats-app-rolls-out-crypto-one-billion/.

Wintour, Patrick. “Margaret Thatcher's Political Legacy Remains Impossible to Avoid.” The Guardian, April 8, 2013. https://www.theguardian.com/politics/2013/apr/08/margaret-thatchers-political-legacy.

Vogel, Kenneth P. “Google Critic Ousted From Think Tank Funded by the Tech Giant.” The New York Times, August 30, 2017. https://www.nytimes.com/2017/08/30/us/politics/eric-schm
]idt-google-new-america.html.

Vogel, Kenneth P. “New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic.” *The New York Times*, September 1, 2017. https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.

Volz, Dustin. “Silicon Valley Mostly Quiet in Internet Surveillance Debate in Congress.” Reuters, July 18, 2017. https://uk.reuters.com/article/us-usa-intelligence/silicon-valley-mostly-quiet-in-internet-surveillance-debate-in-congress-idUKKBN1A32B3.

Waddell, Kaveh. “Is Digital Privacy Becoming a Partisan Issue?” *The Atlantic*, March 7, 2016. https://www.theatlantic.com/technology/archive/2016/03/is-digital-privacy-becoming-a-partisan-issue/472449/.

Wagner, Kurt. “Facebook, Twitter Back Apple CEO Tim Cook in Security Fight With FBI.” Recode, February 18, 2016. https://www.recode.net/2016/2/18/11588026/facebook-twitter-back-apple-ceo-tim-cook-in-security-fight-with-fbi.

Ward, Andrew, Jim Pickard, and Michael Stothard, “Hinkley Go-Ahead After ‘National Security’ Safeguards.” Financial Times, September 15, 2016. https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43.

Weinstein, Mark. “FBI vs Apple: Defining Our Constitutional Future.” Huffington Post, February 19, 2016. https://www.huffingtonpost.com/mark-weinstein/fbi-vs-apple-defining-our_b_9260606.html.

Winter, Brian. “Insight: How U.S. Spying Cost Boeing Multibillion-Dollar Jet Contract,” Reuters, December 20, 2013. https://www.reuters.com/article/us-boeing-brazil-insight/insight-how-u-s-spying-cost-boeing-multibillion-dollar-jet-contract-idUSBRE9BJ10P20131220.

Wittes, Benjamin. *The Lawfare Podcast: Dave Aitel and Matt Tait on How "Everything You Know About the Vulnerability Equities Process Is Wrong."* The Lawfare Podcast, August 27, 2016. https://www.lawfareblog.com/lawfare-podcast-dave-aitel-and-matt-tait-how-everything-you-know-about-vulnerability-equities

Wright, David. “Donald Trump: Apple Should Hack San Bernardino Phone.” CNN, February 17, 2016. https://edition.cnn.com/2016/02/17/politics/donald-trump-apple-encryption-debate/.

Wright, Oliver. “GCHQ's 'Spook First‘ Programme to Train Britain’s Most Talented Tech Entrepreneurs.” The Independent, January 1, 2015. http://www.independent.co.uk/life-style/gadgets-and-tech/news/gchqs-spook-first-programme-to-train-britains-most-talented-tech-entrepreneurs-9953516.html.

Yadron, Danny. “San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance.” The Guardian, March 29, 2016. http://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone.

Yadron, Danny. "'Worth it': FBI Admits It Paid $1.3m to Hack into San Bernardino iPhone." The Guardian, April 21, 2016. http://www.theguardian.com/technology/2016/apr/21/fbi-apple-iphone-hack-san-bernardino-price-paid.

Yadron, Danny, Alistair Barr, and Daisuke Wakabayashi. "Paris Attacks Fan Encryption Debate." The Wall Street Journal, November 20, 2015. http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

"Antenn, Digital Identity Management." RaulWalter, accessed April 30, 2018. https://www.raulwalter.com/government/digital-identity-management/.

"About Us." TechLink, accessed May 3, 2018. http://ukesttechlink.com/about-us/.

"Appeals Court Upholds Constitutional Right Against Forced Decryption." Electronic Frontier Foundation, February 24, 2012. https://www.eff.org/press/releases/appeals-court-upholds-constitutional-right-against-forced-decryption.

"Apple Is Right on Encryption." The Wall Street Journal, March 2, 2016. http://www.wsj.com/articles/apple-is-right-on-encryption-1456877827.

"At Least 14 Dead in California Shooting." BBC News, December 3, 2015. https://www.bbc.com/news/world-us-canada-34987697.

"Building a Seamless Society." Nortal, accessed April 5, 2018. https://nortal.com/.

"Company Overview of Portsmouth Water Limited." *Bloomberg*, October 11, 2017. http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=12505401.

"Core Messages." Brand Estonia, accessed April 5, 2018. https://brand.estonia.ee/principles/core-messages/.

Crypto@berkeley." The Cryptography Group, accessed March 26, 2018. https://crypto.eecs.berkeley.edu/.

Cryptography and Information Security Group." MIT Computer Science & Artificial Intelligence Lab, December 5, 2017, https://crypto.eecs.berkeley.edu/.

"Cyber Security Information Sharing Partnership (CiSP)." NCSC, March 20, 2018. https://www.ncsc.gov.uk/cisp.

"Data Protection." Nortal, accessed April 30, 2018. https://nortal.com/business/data-protection/.

"Digital Agenda Scoreboard Key Indicators." European Commission Digital Single Market, accessed April 23, 2018. https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/visualizations.

"Digitisation." Andmevara, accessed April 30, 2018. https://www.andmevara.ee/en/web/eng/digitisation.

"E-Cadastre." Datel, accessed April 30, 2018. http://www.datel.eu/en/solutions/e-government-solutions/item/232.

"eGovernment." Guardtime, accessed April 27, 2018. https://guardtime.com/solutions/egovernment.

"Estonia and Finland to Develop the X-Road Together." ShowTime, October 6, 2017. https://www.ria.ee/en/estonia-and-finland-to-develop-the-x-road-together.html.

"Estonia Celebrates the Day of Restoration of Independence." Estonian World, August 20, 2016. http://estonianworld.com/life/estonia-celebrates-the-day-of-restoration-of-independence/.

"Estonia Is Trying to Convert the EU to Its Digital Creed." The Economist, July 6, 2017. https://www.economist.com/news/europe/21724831-country-e-residency-wonders-why-others-are-more-sceptical-estonia-trying-convert.

"Estonia to Open the World's First Data Embassy in Luxembourg." e-Estonia, June 2017. https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

"Google Policy Fellowship." Google. https://www.google.com/policyfellowship/hosts.html.

"Government." Roksnet, accessed April 30, 2018. https://www.roksnet.com/government.

"Hinkley Point: UK Approves Nuclear Plant Deal." BBC News, September 15, 2016. http://www.bbc.com/news/business-37369786.

"How Did Estonia Become a Leader in Technology?" The Economist, July 30, 2013. https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology.

"How to Stay in – Manage an EU Company from the UK." e-Residency, accessed April 17, 2018. http://www.howtostayin.eu/.

"How to Tame the Tech Titans," The Economist, January 18, 2018, https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame.

"ID Card." e-Estonia, accessed April 18, 2018. https://e-estonia.com/solutions/e-identity/id-card/.

"Inside the World's Most Advanced Digital Society." Apolitical, July 7, 2016. https://apolitical.co/solution_article/estonia-digital-government-residency/.

"Internet-Based SCADA: the New Era in Communication Technology." Real Time Solutions, March 17, 2008, http://www.rts.com.np/downloads/whatsscada.pdf.

"Introduction to Cryptography." GPGTools, April 13, 2017. https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography

Lobbying Spending Database." OpenSecrets, accessed March 28, 2018. https://www.opensecrets.org/lobby/top.php?showYear=2017&indexType=s

"Lobbying Spending Database - Facebook Inc." OpenSecrets, accessed March 2, 2018. https://www.opensecrets.org/lobby/clientsum.php?id=D000033563&year=2017

"Market Failure." Investopedia, accessed May 9, 2017. http://www.investopedia.com/terms/m/marketfailure.asp.

"Mobile ID Is an Electronic Identity and Digital Signature Solution." Nortal, accessed April 30, 2018. https://nortal.com/government/electronic-identity/mobile-id/

"National and International Policy for Critical Infrastructure Cybersecurity." PETRAS, accessed October 11, 2017. https://www.petrashub.org/portfolio-item/national-and-international-policy-for-critical-infrastructure-cybersecurity/.

"NATO Cyber Defence Fact Sheet." NATO, July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

"Not My Problem: Providing Incentives for Good Behaviour," The Economist, July 14, 2014, https://www.economist.com/special-report/2014/07/14/not-my-problem.

"Not Only Skype: Why a Small Baltic Country in Europe's North-East Is a Hotbed for Start-Ups." The Economist, July 11, 2013. https://www.economist.com/blogs/schumpeter/2013/07/estonias-technology-cluster.

"Overview." Signwise, accessed April 30, 2018. https://signwiseservices.com/#overview.

"Portfolio." Aktors, accessed April 30, 2018. http://www.aktors.ee/en/portfolio.html#xroad.

"Ransomware." Trend Micro, accessed January 16, 2017. http://www.trendmicro.com/vinfo/us/security/definition/ransomware.

"San Bernardino Terror Attack: Police Describe Gun Battle with Terrorist Couple." Fox News, May 26, 2017. http://www.foxnews.com/us/2017/05/26/san-bernardino-terror-attack-terrorists-were-shot-up-to-27-times-during-gun-battle-with-police.html.

"Security and Safety." e-Estonia, accessed April 5, 2018. https://e-estonia.com/solutions/security-and-safety/.

"The Advantages of SCADA for Water/Wastewater Treatment Facilities." Shrader Engineering, March 12, 2012. http://www.shrader.net/news/the-advantages-of-scada-for-water-wastewater-treatment-facilities.

"The Encryption Farce." The Wall Street Journal, April 25, 2016. http://www.wsj.com/articles/the-encryption-farce-1461624399.

"Tony Blair: 'My Job Was to Build on Some Thatcher Policies.'" BBC News, April 8, 2013. http://www.bbc.co.uk/news/av/uk-politics-22073434/tony-blair-my-job-was-to-build-on-some-thatcher-policies.

"UK's Unbalanced Relationship with China." Financial Times, September 22, 2015. https://www.ft.com/content/b18ae09c-611c-11e5-9846-de406ccb37f2?mhq5j=e5.

"# We Break Security to Bring Clarity." Clarified Security. Accessed August 5, 2018. https://www.clarifiedsecurity.com/.

"We Have Built a Digital Society and So Can You." e-Estonia, accessed April 17, 2018, https://e-estonia.com.

"What is a Man-in-the-middle Attack?." Norton, accessed September 1, 2018. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

"X-Road." Cybernetica, accessed April 30, 2018. https://cyber.ee/en/e-government/x-road/