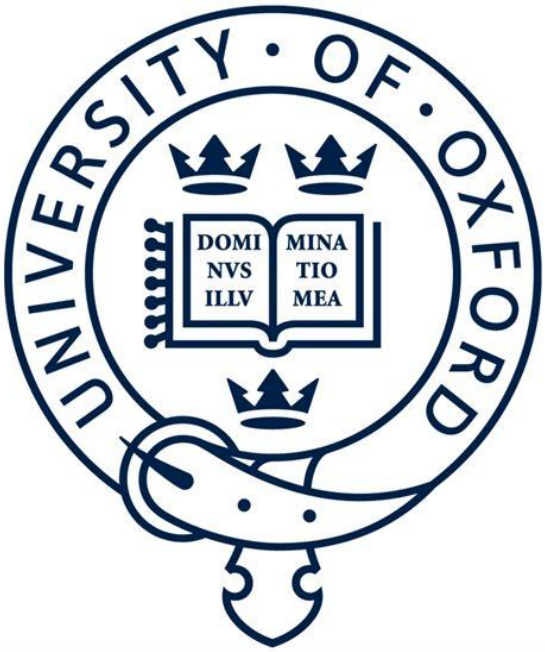
Moral manoeuvres: cybersecurity in Egypt and the Gulf states



Thesis submitted in partial fulfilment of the
requirements for the degree of Doctor of Philosophy in
the Department of Politics and International Relations
at the University of Oxford

August 2018

James Shires
Christ Church College

Word count: 99456

Abstract

Cybersecurity is a complex and contested issue in international politics. The existence of radically different conceptions of cybersecurity is recognised by many scholars in International Relations (IR), but rarely explored outside the cyber 'great powers': the US, the EU, Russia and China. This thesis investigates cybersecurity in Egypt and the states of the Gulf Cooperation Council (GCC), a region between two poles of internet governance that has close military and security ties to the US and Europe *and* authoritarian features more reminiscent of Russia or China. Given this hybrid position, the research question of this thesis is: how can we explain the nature of cybersecurity in Egypt and the Gulf states? This question is not merely academic, as it directly affects the creation of international agreements, laws and institutions, as well as corporate and state surveillance practices.

The thesis argues that cybersecurity is primarily an expert discourse incorporating both technical and value claims. The content of this discourse – *who* cybersecurity protects from *what* – is ambiguous due to both professional incentives and technological characteristics. Relevant actors use this ambiguity to perform what I call 'moral manoeuvres': altering values and technical concepts within this professional discourse for their own ends. I identify four separate moral manoeuvres, which I call alignment, appropriation, manipulation and elision. These manoeuvres are performed by human rights NGOs, government organisations, international surveillance suppliers, and the wider cybersecurity industry respectively. The overall result of these moral manoeuvres is the preservation and even amplification of contradictions and ambiguities present in expert cybersecurity discourses. This thesis makes three original contributions to IR: first, it provides a more nuanced account of the construction of security domains than critical theories of securitisation; second, it explains struggles over values in cybersecurity better than alternative accounts of 'cyber norms'; and third, it presents detailed empirical data on an important region and issue area with few existing treatments.

Acknowledgements

I acknowledge first of all the generosity and insight of my supervisors: Professor Anne Deighton, Dr Lucas Kello, and Professor Todd Hall. Professor Deighton shepherded this project through its first year with constant encouragement and advice gratefully received since then. Dr Kello offered much sage advice and, by inviting me to join first the Cyber Studies Programme and then the Centre for Technology for Global Affairs (CTGA), created the perfect environment in which to write a thesis on technology and IR. Professor Hall provided many insights, improving this thesis immeasurably and seeing in it what I could not. I also thank Professor Edward Keene, my college advisor, for his generous pastoral guidance. I acknowledge the time and intellectual effort given by students and colleagues who read and commented on drafts of this thesis. These include all members of the CTGA, especially Dr Max Smeets, Dr Florian Egloff, and Valentin Weber, and outside the CTGA Professor Kate Millar, Lilly Muller, Josie Kaye, Cate Laporte-Oshiro, and Anette Stimmer. Many thanks to all of you.

This work has benefited from feedback to presentations given at the Centre for Doctoral Training in Cyber Security, the DPIR DPhil seminar, and at successive conferences of the International Studies Association, the International Communications Association, and the British Society for Middle East Studies. I would especially like to thank Monterey Naval College, University of Toronto, London School of Economics and King Saud University for their invitations to present this work. I am also grateful to the staff at the CTGA, DPIR, and Economic and Social Research Council (ESRC) for their kind and efficient support. I would also like to thank bodies who supported the research of this thesis through various grants: ESRC, CTGA, DPIR, Christ Church College, and the Anglo-Omani Society.

Thank you to all those who helped me while on fieldwork, whether with contacts, interviews, a place to stay, dinner, a chat over coffee or all of the above. This thesis would have been impossible without the curiosity, kindness, and generosity of all those I met working in cybersecurity in Egypt and the Gulf states, whose passion for their subject and their values never ceased to be humbling. Finally, I thank my family and Annabel for their unwavering support in every way.

Contents

Tables and figures

Note on transliteration and interviews

Arabic transliterations use a simplified version of the transliteration scheme recommended by the International Journal of Middle East Studies, with all diacritical marks omitted. Widely used transliterations not following this scheme are retained for common proper nouns.

Conference presentations and conversations are referenced with the abbreviated name of the conference in brackets after the quotation, based on Table 1. Quotations from anonymous interviews are allocated a random interview number and referenced in brackets after the quotation, e.g. (I-15). Table 3 provides further details (still anonymised) of the interviewees according to their interview number. This interview number is deliberately different to that used in other works referencing the same sources. I use the pronoun ‘they’ to refer to all interviewees to avoid identification by gender.

List of acronyms and abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
Arab Convention	Arab Convention on Combating Information Technology Crimes
ASEAN	Association of South East Asian Nations
BBC	British Broadcasting Corporation
BD	Business Development
BIS	Bureau of Industry and Skills (US)
Budapest Convention	Council of Europe Convention on Cybercrime
CCL	Commerce Control List (US)
CCM	Computers Cleaned per Mille
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIO	Chief Information Officer
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CNI	Critical National Infrastructure
CNN	Cable News Network
CTO	Chief Technology Officer
DDOS	Distributed Denial of Service
DEWA	Dubai Electricity and Water Authority
DIT	Department of International Trade (UK)
DPI	Deep Packet Inspection
EAR	Export Administration Regulations (US)
ECO	Export Control Organisation (UK)
EFF	Electronic Frontier Foundation
EMEA	Europe, Middle East and Africa
ESCWA	Economic and Social Commission for Western Asia
EU	European Union
FBI	Federal Bureau of Investigation (US)
FCPA	Foreign Corrupt Practices Act (US)
G77	Group of 77
GCC	Gulf Cooperation Council
GCHQ	Government Communications Head Quarters (UK)
GGE	Group of Governmental Experts
GISEC	Gulf Information Security Expo and Conference
High Council	High Council for Cyber Security (Egypt)
HR	Human Resources
HT	Hacking Team
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICT	Information Communications Technologies
IGF	Internet Governance Forum
IMPACT	International Multilateral Partnership Against Cyber Threats

IP	Internet Protocol or Intellectual Property
IR	International Relations
ISO	International Standards Organization
ISP	Internet Service Provider
ISSA	Information Systems Security Association
IT	Information Technology
ITA	Information Technology Authority
ITU	International Telecommunications Union
KACST	King ʿAbdullah City for Science and Technology
LAS	League of Arab States
MCIT	Ministry of Communications and Information Technology
MFA	Ministry of Foreign Affairs
MOD	Ministry of Defence
MOI	Ministry of Information or Interior
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre (Saudi Arabia)
NESA	National Electronic Security Authority (UAE)
NGO	Non-Governmental Organisation
NIST	National Institute for Standards and Technology (US)
NSA	National Security Agency (US)
OECD	Organisation for Economic Cooperation and Development
OIC	Organisation of Islamic Cooperation
ONI	Open Net Initiative
OTT	Over-The-Top (web applications)
OWASP	Open Web Application Security Project
QNA	Qatar News Agency
RAT	Remote Access Tool
SCAF	Supreme Council of the Armed Forces (Egypt)
SIGINT	Signals Intelligence
SOC	Security Operations Centre
STEM	Science, Technology, Engineering and Mathematics
TRA	Telecommunications Regulatory Authority/Agency
TRD	Technical Research Department (Egypt)
TTP	Techniques, Tactics and Procedures
UAE	United Arab Emirates
UK	United Kingdom
UML	US Munitions List
UN	United Nations
UNESCO	UN Educational, Scientific and Cultural Organization
US	United States of America
VOIP	Voice Over IP
VPN	Virtual Private Network
Wassenaar	Wassenaar Arrangement on Dual-Use Technologies
WCIT	World Congress on Information Technology
WSIS	World Summit for the Information Society

Chapter 1. Introduction

1.1 Motivation

On 2 and 3 April 2012, a 'Cyber Defence Summit' was held in the Grand Hyatt Hotel in Muscat, Oman. The summit was organised by the Oman Information Technology Authority (ITA) and sponsored by several defence multinationals and the cybersecurity arm of the International Telecommunications Union (ITU), among others.[1] It featured speakers from the North Atlantic Treaty Organisation (NATO) and the US Federal Bureau of Investigation (FBI).[2] This was the second Cyber Defence Summit in the Gulf; the first had taken place in the United Arab Emirates (UAE) the year before, and it would reoccur annually as the "Arab Region Cyber Security Summit", including one in Egypt in 2016. The blurb of the 2012 meeting was clear about its aims:

> The Cyber Defence Summit is gathering the key regional stakeholders in Muscat, Oman to discuss and explore the heightened importance of cyber security in the region. Under the theme 'Defending your virtual borders' — the invitation-only initiative is focused on protecting the virtual boundaries of the Middle East.[3]

Three months later, on 25 July 2012, an organisation at the University of Toronto, Citizen Lab, released a report detailing the use of a digital surveillance tool named Finfisher in Bahrain.[4] The tool – described as malicious software, or 'malware' by Citizen Lab – had been used to obtain information from the devices of pro-democracy activists in Bahrain, where there had been extensive protests and violent responses from government security forces since the 'Arab Spring' in 2011. Other investigations found that Finfisher had been trialled in Egypt just before the January 2011 revolution.[5] Finfisher was later observed by Citizen Lab in many countries, including Oman, Qatar,

[1] BAH Press release, 'Booz Allen Hamilton Aims to Protect Middle East', Petroleum Africa, 20 March 2012, https://perma.cc/D27N-3JXD.
[2] Conrad Prabhu, 'Concern over Cyber Attacks', *Oman Daily Observer*, 20 March 2012, https://perma.cc/H69G-49R5.
[3] Prabhu.
[4] Bill Marczak and Morgan Marquis-Boire, 'From Bahrain with Love: Finfisher's Spy Kit Exposed?' (Citizen Lab, 25 July 2012).
[5] Karen McVeigh, 'British Firm Offered Spying Software to Egyptian Regime – Documents', *The Guardian*, 28 April 2011, https://perma.cc/GCV9-DUJS.

Saudi Arabia and the UAE, with its likely purchaser and user in all cases being their respective governments.[6] Concluding their analysis of Finfisher in Bahrain, Citizen Lab issued a call to the cybersecurity community, saying that "we strongly urge antivirus companies and security researchers to continue where we have left off" in investigating government uses of surveillance tools like Finfisher.[7]

Three weeks later, on 13 August 2012, the UAE issued an updated Federal Law on Combating Cybercrimes. This law increased both the number of offences and severity of penalties from the previous cybercrime law of 2006. Both laws included a wide definition of 'content crimes': penalties for posting or messaging about certain topics online or facilitating such posts by operating social media platforms or websites.[8] The new law mirrored similar laws in the rest of the Gulf, either already in place or brought in soon afterwards, as well as draft laws discussed in Egypt throughout 2015 and 2016. The scope of the UAE law was very broad. Article 24 stated that:

> Shall be punished by temporary imprisonment and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams: whoever establishes or administers or runs a website or publishes on a computer network or any information technology means which would promote or praise any programs or ideas which would prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace or prejudice the public order and public morals.[9]

Three days later, on 16 August 2012, malware known as 'Shamoon' spread through the business networks of the Saudi national oil company, Saudi Aramco, and wiped data from around 30,000 computers. A few weeks later the Qatari gas company RasGas – the largest exporter of liquid natural gas in the world - was also affected. Shamoon was eventually attributed to the Iranian government.[10] According to Saudi officials, the aim was to "stop the flow of Saudi oil".[11] Shamoon was described as a "wake-up call" by a senior US cybersecurity official, who added that "a similar

[6] Bill Marczak et al., 'Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation' (Citizen Lab, 15 October 2015).
[7] Marczak and Marquis-Boire, 'From Bahrain with Love: Finfisher's Spy Kit Exposed?'
[8] This approach echoes the concept of 'information security' rather than 'cybersecurity' prevalent in many states, including China and Russia. For a detailed discussion, see Chapter 3, Section 3 and Chapter 7, Section 2.
[9] Government of the UAE, 'Federal Decree-Law No. (5) of 2012 On Combating Cybercrimes' (Official Gazette, Issue 540 (unofficial English translation), 13 August 2012).
[10] This attribution was a convoluted process: see Chapter 5, Section 2.
[11] Wael Mahdi, 'Saudi Arabia Says Aramco Cyberattack Came From Foreign States', *Bloomberg*, 9 December 2012, https://perma.cc/NWA4-46LT.

attack on our critical infrastructure networks could have grave effects on financial markets, communication networks, and health and safety services".[12] The US Defence Secretary cited it in a speech warning of a "cyber Pearl Harbor", and it was interpreted by some in the US media as retaliation for previous cyber operations against Iran by the US and Israel.[13] Shamoon has subsequently become a standard reference for "destructive cyber-attacks" in International Relations (IR).[14]

The four events above, which occurred within months, weeks, or even days of each other, were clearly seen by their participants as part of cybersecurity. However, there are substantial differences between the conceptions of cybersecurity encapsulated in each event. The Cyber Defence Summit focused on military threats, looking to defend "virtual boundaries" in the way that armed forces traditionally defend physical borders. In contrast, Finfisher was described by its discoverers as a cybersecurity threat to privacy and individual human rights, although its government purchasers saw it as a crucial tool for national security investigations. The UAE cybercrime law offered yet another conception of cybersecurity, criminalising online comments as cybersecurity threats to "national unity" and "public morals" among others. Finally, the Shamoon attack was taken to herald the advent of 'destructive' malware, showing that advanced threats could severely damage the physical operations of companies and governments.

Notwithstanding larger social, technological and institutional networks, all four events above also centre around Egypt and the six states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE. This region within the wider Middle East is the subject of this thesis for two reasons. First, this thesis examines Egypt and the Gulf states *together* through a regional lens, albeit with significant internal differences, because there is a distinct professional cybersecurity community across these states that shares tools, organisations, people and practices.

[12] Infosecurity, 'Saudi Aramco Cyber Attacks a "Wake-up Call", Says Former NSA Boss', Infosecurity Magazine, 8 May 2014, https://perma.cc/NXT5-3J57.
[13] Elisabeth Bumiller and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.', *The New York Times*, 11 October 2012, https://perma.cc/F5ZH-YSSV; Nicole Perlroth, 'Cyberattack on Saudi Oil Firm Disquiets U.S.', *The New York Times*, 23 October 2012, https://perma.cc/CP22-JCHM.
[14] Christopher Bronk and Eneken Tikk-Ringas, 'The Cyber Attack on Saudi Aramco', *Survival* 55, no. 2 (1 May 2013): 81–96.

Second, this thesis examines Egypt and the Gulf states instead of the usual cyber 'great powers' of the US, Russia, China, or the European Union, because Egypt and the Gulf states all occupy a hybrid position in international internet governance, with close military and security ties to the US and Europe on the one hand and authoritarian features more reminiscent of Russia or China on the other. Consequently, as the four events above illustrate, these states are the site of radically different conceptions of cybersecurity.

Many analyses of cybersecurity in international politics focus on only one of these conceptions of cybersecurity, thereby missing the broader picture. In contrast, the motivation for this thesis is to make sense of these drastically divergent conceptions of cybersecurity, all present within such a short space of time and in a small geographical region. I seek to understand how and why these different conceptions of cybersecurity collide, overlap, and interact. My account of the emergence of cybersecurity in Egypt and the Gulf states treats conceptions of cybersecurity not as objective truths, nor as distinct and unconnected realms, but instead as crafted by specific individuals and groups in the pursuit of social, political and economic goals. This thesis thus sheds light on the organisations, practices and rationales behind the continuous making and remaking of cybersecurity itself.

This is not merely an academic issue, as how cybersecurity is defined—what its objectives, limits, moral and ethical obligations are —has major economic, political, and social consequences. The policy stakes are high, as struggles over what constitutes cybersecurity in this region directly affect the implementation of international agreements and the creation of new laws and institutions at national and international levels, as well as questions of corporate and state responsibility for the surveillance of individual citizens. In an echo of colonial-era dynamics, Egypt and the Gulf states are now located at a confluence of global flows of data, capital, arms, and expert practices, creating a highly complex and important environment in which to study the nature of cybersecurity.

1.2 Argument

The research question of this thesis asks: how can we explain the nature of cybersecurity in Egypt and the Gulf states?[15] In brief, this thesis argues that cybersecurity is not a single monolithic entity, but a syncretic blend of different conceptions within an ambiguous professional discourse. These conceptions interact through what I call the 'moral manoeuvres' of actors who seek to either mould cybersecurity to promote a specific value or keep its content ambiguous for their own benefit.

The argument of this thesis begins with the claim that cybersecurity is primarily a professional discourse created and maintained by cybersecurity 'experts' (a term that will be investigated in detail in later chapters). This professional discourse, as a *security* discourse, is essentially value-based. Values are abstract concepts with connotations of good or worth, such as security, freedom, justice, happiness, privacy, and so on. Values form groups or clusters due to many factors including conceptual similarities, institutional mechanics and prevailing interests. For example, a wide range of values are clustered together as 'human rights', due to contingent historical associations, similar philosophical foundations, and their incorporation into dominant global power structures in the second half of the twentieth century.[16] Crucially, the cybersecurity professional discourse, as a *cyber* discourse, also combines values with factual and technical claims about the use and behaviour of digital technologies, often using specialist terminology to do so. These claims add meaning to abstract values, mobilising them and making them intelligible in cybersecurity.

The result is a generic 'organisational' conception of cybersecurity, which incorporates a cluster of values aiming to protect commercial and government organisations from a range of threats including hacktivism, cybercrime, and cyber espionage. However, the organisational conception of cybersecurity is both *malleable*, in that it can easily be altered to accommodate new situations, and

[15] The 'we' here refers to academic researchers in IR. For an account of the relationship of this community to that studied by the thesis see Chapter 4, Section 1 and Chapter 10, Section 3.

[16] Jack Donnelly, *Universal Human Rights in Theory and Practice* (Ithaca: Cornell University Press, 2002); Paul Gordon Lauren, *The Evolution of International Human Rights: Visions Seen* (Philadelphia: University of Pennsylvania Press, 2011); Charles R. Beitz, *The Idea of Human Rights* (Oxford: Oxford University Press, USA, 2011); Daniel C. Thomas, *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism.* (Princeton, N.J: Princeton University Press, 2001); Mary Ann Glendon, *A World Made New* (New York: Random House USA Inc, 2002).

ambiguous, in that it is often not clear who or what is the exact threat or vulnerable entity to which it refers. This is a result of both technological characteristics (as digital technologies can be used in a variety of ways) and professional incentives (as experts market their cybersecurity services and solutions to different audiences).

The ambiguous nature of professional cybersecurity discourse enables actors to perform what I call 'moral manoeuvres': the alteration of values and technical concepts for their own ends.[17] As the cybersecurity professional discourse includes both abstract values *and* factual or technical claims, moral manoeuvres involve the renegotiation of these facts and values and the relationship between them. The original concept of moral manoeuvres is the keystone of this thesis and will be defined further in relation to existing literature in Chapter 2.

Moral manoeuvres engage with multiple clusters of values in cybersecurity. As well as the organisational cluster of values dominating the professional discourse, there is also a 'rights-based' cluster of values in cybersecurity, which focuses on threats to freedom of expression and rights against torture and mistreatment. There is also a further cluster of values around an expansive definition of national security that targets a wide range of political speech online. Some moral manoeuvres alter values and technical claims mainly within one value cluster, while others move fluidly between them.

I distinguish between two types of moral manoeuvres according to the motivation of the actor performing them, as either *invested* or *agnostic*. Invested actors seek to promote a particular value or cluster of values. In contrast, agnostic actors seek to maintain the ambiguity of cybersecurity discourse between different values or clusters of values to achieve a separate goal. For the actors considered in this thesis, such goals are economic, concerned with profit, although there are other possibilities noted in Chapter 2.

I identify four moral manoeuvres using the distinction between invested and agnostic actors above. First, actors invested in a particular value or cluster of values can seek to reframe their value preferences to fit existing discourses, which I call *alignment*. Second, invested actors can do the

[17] Following IR terminology more generally, actors are corporate, composed of many parts. States, companies, NGOs, and professional bodies are actors in the IR sense.

opposite and seek to expand these discourses to fit their value preferences, which I call *appropriation*. Third, actors who are agnostic between different values or clusters of values can seek to exploit the contradictions between those values within a discourse, which I call *manipulation*. Fourth, agnostic actors could also do the opposite and minimise these contradictions, which I call *elision*. This list does not exhaust the possible space of moral manoeuvres, although it does represent four intuitive ways in which actors can renegotiate ambiguous technical and value claims in an issue area. The overall result of these moral manoeuvres is a cybersecurity discourse that retains and amplifies existing ambiguities and contradictions.

In this thesis, I investigate all four moral manoeuvres above: alignment, appropriation, manipulation and elision. I argue that these moral manoeuvres are performed by non-governmental organisations (NGOs), states, international surveillance suppliers, and the wider cybersecurity industry respectively. The first two actors are characterised by very different invested motivations, while the latter two are characterised by agnostic economic motivations. All four actors are cybersecurity 'experts', although their expertise is contested in ways that will be interrogated throughout the thesis. I now provide an overview of each moral manoeuvre in turn.

First, human rights NGOs *aligned* technical and discursive characteristics of the rights-based conception of cybersecurity with the organisational conception, so that threats to individual rights were reframed in the terminology of threats to organisations. These actors, especially the Canadian NGO Citizen Lab, used this alignment to highlight the association of surveillance technologies with human rights violations *as a cybersecurity issue*, as in the case of Finfisher above. They used their position as cybersecurity experts, rather than pure advocacy groups, to advise on the amendment of the Wassenaar Arrangement, an international arms control agreement for dual-use items, to include such technologies. The motivation for this moral manoeuvre was invested, as it sought to promote human rights values in cybersecurity, and its scope was between the organisational and rights-based value clusters.

Second, government departments in Egypt and the Gulf states *appropriated* the organisational conception of cybersecurity to limit criticism and political debate. This moral manoeuvre occurred as part of institutional struggles in which interior ministries and security

services assumed cybersecurity responsibility from telecoms and IT departments. This struggle led to a conception of cybersecurity as concerned with the threat of critical comments on social media, and the adoption of laws across Egypt and the Gulf states that expanded the concept of 'cybercrime' from its original focus on economic loss to political speech online. The motivation for this moral manoeuvre was also invested, as it was premised on an expansive definition of national security. Its scope was limited to the organisational and national security value clusters, rarely engaging with human rights values.

Third, international surveillance suppliers *manipulated* both organisational and human rights values for economic gain. These suppliers incorporated the risk of human rights violations into their sales procedures partly as a strategic initiative against the work of Citizen Lab, both before and after the amendment of the Wassenaar Arrangement. Both companies and exporting states such as the UK created institutions to assess the 'misuse' of surveillance technologies, which provided an appearance of responsible businesses and states but incorporated sufficient flexibility to continue prior sales. The motivation for this moral manoeuvre was agnostic, aiming to increase sales of surveillance equipment rather than stemming from any commitment to national security or human rights *per se*. Its scope was wide, ranging regularly between organisational, national security and rights-based value clusters.

Fourth, the wider cybersecurity industry *elided* differences between different organisational values, also for economic gain. Several cybersecurity actors, including specialised cybersecurity companies, local surveillance resellers, and national telecoms companies, operate in both national surveillance and commercial cybersecurity environments and yet are not subject to export restrictions or human rights pressures like those incorporated into the Wassenaar Arrangement. These actors created what I call 'portable' technical concepts to assist the transfer of technologies between these two environments, obscuring the difference between the relevant values in each one. The motivation for this moral manoeuvre was also agnostic, aiming to sell cybersecurity solutions and services outside surveillance industries. Unlike the manipulation of international suppliers, its scope was mainly limited to the organisational value cluster, with only occasional acknowledgement of human rights values.

Specifying these four moral manoeuvres enables us to state more fully the answer to the research question posed above: how can we explain the nature of cybersecurity in Egypt and the Gulf states? Cybersecurity in this region is not a single monolithic entity, but a syncretic blend of different conceptions (organisational, rights-based, or drawn from an expansive interpretation of national security) within an ambiguous professional discourse. These conceptions of cybersecurity interact through the moral manoeuvres – the alteration of and renegotiation between values and technical concepts – of relevant actors who seek to either mould cybersecurity to promote a specific value (i.e. they are invested) or keep its content ambiguous for their own benefit (i.e. they are agnostic). The overall result of these moral manoeuvres is the preservation and even amplification of the contradictions and ambiguities present in the expert cybersecurity discourse.

Each moral manoeuvre has clear consequences for cybersecurity and international politics more broadly. Alignment led to the amendment of the Wassenaar Arrangement, appropriation created a raft of new cybersecurity laws and institutions at both national and international levels, manipulation involved the formation and exploitation of structures to judge the 'misuse' of surveillance equipment, and elision changed the character of cybersecurity expert practices themselves. The moral manoeuvres examined in this thesis are therefore important not only for IR theory, but are also highly relevant to cybersecurity practitioners, policy-makers, and individuals.

This thesis uses several qualitative methods to investigate the four moral manoeuvres above, including: discourse analysis of national strategies, cybersecurity laws and professional documents in English and Arabic; interviews with cybersecurity professionals; and ethnographic participant observation in cybersecurity conferences. These methods and the data used are detailed in Chapter 4. Finally, all four moral manoeuvres occur between 2011 and 2017. This short time frame has a clear benefit, as it allows close examination of specific actors, decisions and events, and its boundaries are justified in detail in Chapter 3. However, the negative corollary is that I can only briefly examine the longer-term patterns behind the events considered here, and I gesture to these trends in Chapter 5.

1.3 Contributions

This thesis contributes a novel account of value-based interaction to IR theory, including the original concept of moral manoeuvres. This account is inspired by critical and constructivist approaches to power, knowledge, values and technology, and addresses key gaps or tensions in both approaches. These contributions are explored in detail in the following chapter, and I summarise the key points here.

Scholars in critical security studies have produced many insightful works in cybersecurity, deploying the concept of 'securitisation' to show how cybersecurity is contingently constructed by speaking 'cybersecurity' to an audience in a specific context. However, critical cybersecurity studies have three main shortcomings. First, they adopt from securitisation theory a binary focus on the concepts of threat and victim (or 'referent object'), thereby discounting the wide range of values present *within* security discourses. Second, although critical treatments of cybersecurity have a sophisticated understanding of power in international politics, they rarely recognise the implications of that understanding on values: namely, that values are simultaneously both objects within a strategic calculation *and* goals that direct the behaviour of actors. Finally, critical cybersecurity studies have imported many productive ideas from science and technology studies (STS) about the importance of objects – both physical and digital – in security practices. However, this close relationship with STS leads to a danger already noted by some STS scholars, in that 'flattening' the relationships between actors and objects reduces the space for moral agency in international politics.

All three of these issues are addressed by the concept of moral manoeuvres. First, the concept of moral manoeuvres takes critical cybersecurity studies beyond the twin frames of securitisation and counter-securitisation. Cybersecurity is, by definition, a successful securitisation, and yet the professional discourse in Egypt and the Gulf states retains substantial ambiguity towards its referent. Rather than a pure polarisation of what securitisation theory calls 'normal politics', this ambivalent professional discourse enables the simultaneous co-existence of a range of conceptions of cybersecurity not captured by securitisation theory. Second, the distinction between invested and agnostic actors directly explains the ways in which value judgements are strategically manipulated

for both value-based and economic reasons. By doing so, it builds a bridge between critical approaches to power and similar themes in revisionist strategic studies treatments of cybersecurity. Third, and finally, the concept of moral manoeuvres highlights exactly how moral agency functions in a highly technological issue area, and the role of digital and physical objects in shaping both practices and values.

Constructivist work on norms in IR, and especially work on 'cyber norms', has also been a key source of inspiration for this thesis. Many scholars have argued that cybersecurity is structured by cyber norms, including the Wassenaar Arrangement mentioned above and the Council of Europe's Budapest Convention on Cybercrime. However, the status and influence of cyber norms is the subject of significant debate, including over whether 'positive' norms restricting cyber 'weapons' are outweighed by 'negative' norms permitting many other kinds of hostile activity between states, and even whether there has been an 'end of cyber norms' after the collapse of UN cybersecurity discussions in 2017. Many scholars point to the problems of contrasting value systems and differences in underlying values in the formation of cyber norms, but their focus on the norms themselves prevents them from analysing these values in detail.

This debate mirrors the development of norm theories in IR more generally, as scholars have argued that norms across issue areas should be seen as constantly evolving processes rather than clear rules or principles. This is a key tension in norm studies: the more the possibility for change and contest over a norm is emphasised, the less coherent or norm-like the norm itself becomes. In other words, in order to take account of the instrumental quality of values in international politics the language of norms has been stretched beyond what good faith would permit.

The concept of moral manoeuvres alleviates these difficulties in norm studies by providing an alternative theoretical vocabulary in which to analyse the role of values in international politics. It has two main advantages. First, it allows the specification of several simultaneous alterations to values without requiring a norm as the focal point. Although the Wassenaar Arrangement and Budapest Convention appear regularly in the empirical chapters of this thesis, I show that these norms are only one part of a whole 'dense normative web' in which actors resist, reinterpret and adapt a range of values. Consequently, agnostic actors who are not invested in specific value clusters

can nevertheless shape the articulation of norms just as much as the invested actors on which norm studies often focus. Second, although the congested value space of cybersecurity means that no single actor can refashion cybersecurity entirely in their image, the combination of these four moral manoeuvres *does* redraw the boundaries and centre of gravity of the issue area overall. The shifting reproduction of issue areas is often underplayed by norm studies to focus on the persistent effect of rules over time. In contrast, the argument here emphasises that moral manoeuvres redefine cybersecurity itself.

The final contribution of this thesis is empirical rather than theoretical. This thesis puts forward a vast amount of new empirical data on cybersecurity in Egypt and the Gulf states, a region in which the issue of cybersecurity has not previously been studied in IR aside from a few short articles. In order to make the argument above, this thesis draws on a wide range of previously unseen primary and secondary sources, including leaked documents from surveillance suppliers, technical documents analysing cybersecurity incidents, cybersecurity laws and media reports in English and Arabic, conference presentations and materials, and interviews. This empirical data greatly advances the study of cybersecurity outside the cyber 'great powers' of the US, Europe, Russia and China, demonstrating that extensive 'on the ground' empirical research is not only possible in sensitive and technical topics like cybersecurity but also – when combined with a theoretical perspective building on both IR theory and Middle East studies - is highly fruitful in revealing the multifaceted nature of cybersecurity discourses emerging worldwide.

While this thesis puts forward the concept of moral manoeuvres in the context of cybersecurity in Egypt and the Gulf states, the theoretical apparatus could be used more widely in cybersecurity and in other issue areas in IR where there is an ambiguous and influential expert discourse. In the thesis conclusion, I consider some of these applications, focusing within cybersecurity on other regions with a hybrid position in global internet governance, and outside cybersecurity on the issue areas of climate change and artificial intelligence.

1.4 Structure

I now provide a brief outline of the structure of the thesis. It is split into two parts: the first part provides the necessary background to the moral manoeuvres performed in cybersecurity in Egypt and the Gulf states, and the second part details the moral manoeuvres themselves.

Chapter 2 provides the theoretical basis for the three key claims of this thesis introduced above: the central role of an ambiguous expert discourse, the concept of moral manoeuvres itself, and the classification of moral manoeuvres using a distinction between invested and agnostic actors. It argues that these claims both build on and constitute an original contribution to critical cybersecurity studies and literature on cyber norms in IR.

Chapter 3 argues that cybersecurity can be usefully studied through a regional lens and that Egypt and the Gulf states constitute a region for cybersecurity. Although, at first sight, the global digital networks underpinning cybersecurity suggest that it is unsuited to a regional analysis, IR theories of regions can be applied to cybersecurity. I use these theories to specify the geographical boundaries of this thesis, excluding other parts of the Middle East which are cybersecurity centres in their own right, and its temporal boundaries, placing the beginning of the empirical analysis at the Arab Spring in 2011 and the end at the Qatar crisis in 2017. This chapter then considers differences in four areas: state formation, communications technologies, human rights, and political developments 2011-2017. Finally, this chapter details the hybrid position of Egypt and the GCC states in international cybersecurity governance, arguing that Egypt and the GCC espouse neither a 'cyber sovereignty' nor a 'multistakeholder' model due to their longstanding association with the ITU on the one hand and close security links with Western states on the other. This creates a complex and contradictory set of pressures on cybersecurity in the region.

Chapter 4 examines the cybersecurity professional community that is the source of the ambiguous discourse underpinning the argument of this thesis. This thesis uses qualitative methods to access this professional community, including discourse analysis, interviews with cybersecurity professionals in government and private sector, and ethnographic participant observation in cybersecurity conferences. This chapter begins with an overview of these conferences, which are an

anchor for all three methods employed in this thesis. It then details the methods themselves and concludes with an overview of key characteristics of the professional community including qualifications, nationality, and gender. This chapter argues that the ambiguity of the professional discourse is not only inherited through the broader genealogy of cybersecurity but is also a result of the complexity of the expert identities present in this regional community.

Chapter 5 turns to the professional discourse itself, and analyses key cybersecurity events in Egypt and the Gulf states to establish the generic 'organisational' conception of cybersecurity that is foundational to this discourse. It begins by tracing the lineage of cybersecurity in this region through lenses of cyberterrorism and cybercrime throughout the 2000s, and then focuses on one cybersecurity event in particular: the cyberattack against Saudi Aramco known as Shamoon, sketched briefly in the opening paragraphs of this introduction. Finally, it broadens the analytical lens to include other cybersecurity events in the main period treated by this thesis, including key instances of hacktivism and cyberespionage. This chapter argues that the range of events in the expert discourse due to both professional incentives and technological characteristics adds to the ambiguity central to this thesis.

In Part 2, Chapters 6-9 detail in turn the four moral manoeuvres above. Chapter 6 examines the moral manoeuvre of alignment, performed by NGOs outside Egypt and the Gulf states due to the conflicted orientation towards human rights values within the regional professional community. Chapter 7 examines the moral manoeuvre of appropriation, performed by state organisations in Egypt and the Gulf states, specifically ministries of interior and security agencies. Chapter 8 examines the moral manoeuvre of manipulation, performed by surveillance suppliers to these states including European and US defence companies and the exporting states themselves. Finally, Chapter 9 examines the moral manoeuvre of elision performed by the cybersecurity industry itself, including cybersecurity companies and telecoms companies with successful cybersecurity businesses.

Chapter 10 concludes. It summarizes the contributions above and makes cautious predictions regarding future developments of cybersecurity in Egypt and the GCC. It also addresses the limitations of this thesis, its scope and methodology. It then explores the implications of this thesis for practitioners and suggests possible applications of concepts outlined here to other topics and regions.

PART 1: UNDERSTANDING CYBERSECURITY

Chapter 2. Theories

Cybersecurity is widely recognised as a new and important issue in IR, and it has attracted attention from diverse theoretical perspectives. Pathbreaking works have analysed cybersecurity from a broadly realist or mainstream strategic studies standpoint.[18] Such works generally view cybersecurity as centred on a specific technological innovation – the cyber 'weapon' – which has new properties, and which could be used in 'cyberwar' or change international order altogether.[19] Other scholars have evaluated the relevance of existing strategic theory to cybersecurity by deploying a range of analogies, including questioning the common characterisation of cyberspace as a military 'domain' akin to those of air, land, sea or space.[20] This thesis follows such work in treating cybersecurity as a distinct issue area within international politics. However, this thesis also builds on critical and constructivist approaches to cybersecurity, in addition to the strategic studies literature above. In this chapter, I expand on the summary in the introduction to show how this thesis is an original contribution to both critical cybersecurity studies and work on 'cyber norms' in IR, by elaborating my approach in contrast to these existing literatures.

This chapter has three sections, each placing a key tenet of the thesis argument within the wider literature. The first section establishes the premise that cybersecurity is primarily an ambiguous professional discourse combining both technical and value claims, showing how this claim contributes to critical theories of expertise in international politics. The second section defines moral manoeuvres, the key concept of this thesis, showing how this concept overcomes shortcomings of both securitisation theory as applied to cybersecurity and theories of cyber norms. The third

[18] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009); Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012).
[19] Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35, no. 1 (1 February 2012): 5–32; John Stone, 'Cyber War Will Take Place!', *Journal of Strategic Studies* 36, no. 1 (1 February 2013): 101–8; Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38, no. 2 (1 October 2013): 7–40; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017); Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 42, no. 1–2 (16 February 2017): 1–28; Thomas Rid, *Rise of the Machines: The Lost History of Cybernetics* (Scribe UK, 2017).
[20] Joseph S. Nye, 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly* 5, no. 4 (2011): 18; David J. Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue* 44, no. 2 (1 April 2013): 147–64; George Perkovich, *Understanding Cyber Conflict: Fourteen Analogies*, ed. Vice President for Studies George Perkovich (Washington, DC: Georgetown University Press, 2018).

section fleshes out the claim that four moral manoeuvres can be distinguished based on what I call the invested or agnostic motivation of relevant actors. It first shows how the invested/agnostic distinction builds on critical approaches to power and strategy to cut across traditional IR distinctions between normative and self-interested action, and then shows how the typology of four moral manoeuvres is an important supplement to theories of norm entrepreneurship and contestation.

2.1 An ambiguous professional discourse

This section argues that critical views of expert practice in general, and cybersecurity expertise in particular, provide good grounds for asserting that cybersecurity professional discourse is deliberately and inherently ambiguous even prior to the empirical analysis in Chapter 5. This is due to professional incentives, technological characteristics and the ubiquitous concept of risk.

Experts and expert knowledge are most commonly understood in IR through the lens of 'epistemic communities', in a term coined by Haas.[21] These views of expertise focus not on expert knowledge in a static, codified form, but on expert *practice* and *performance*. Practices are defined as "socially meaningful patterns of action, which, in being performed more or less competently, simultaneously embody, act out, and reify background knowledge and discourse in and on the material world".[22] Expert practices are important for IR because they form the factual basis for political action, feeding into assumptions made by all political actors about how the world works.

This view of expertise as fields of practice implies that structural and productive forms of power are not only wielded by experts as a cohesive group, but also shape the relationships between and character of experts themselves.[23] Rather than simply importing expert knowledge from their

[21] Peter M. Haas, 'Introduction: Epistemic Communities and International Policy Coordination', *International Organization* 46, no. 1 (1992): 1–35; Mai'a K. Davis Cross, 'Rethinking Epistemic Communities Twenty Years Later', *Review of International Studies* 39, no. 01 (January 2013): 137–160; Christian Bueger, 'From Expert Communities to Epistemic Arrangements: Situating Expertise in International Relations', in *The Global Politics of Science and Technology - Vol. 1*, ed. Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, Global Power Shift (Springer Berlin Heidelberg, 2014), 39–54.
[22] Emanuel Adler and Vincent Pouliot, eds., *International Practices* (Cambridge; New York: Cambridge University Press, 2011), p.6.
[23] Michael Barnett and Raymond Duvall, 'Power in International Politics', *International Organization* 59, no. 1 (2005): 39–75.

academic or professional discipline into problems of societal and political importance, experts conduct what Seabrooke terms 'epistemic arbitrage'. This is where experts "mediate between knowledge pools for strategic advantage and, if successful, they can become the 'arbiters' on what knowledge and practices are most influential".[24] In the words of legal scholar David Kennedy:

> Expert knowledge is human knowledge: a blend of conscious, semiconscious and wholly unconscious ideas, full of tensions and contradictions, inhabited by people who have projects and who think, speak and act strategically. Style and role count as much as content.[25]

In his analysis of international human rights law, Kennedy argues that expert performance is flexible and ambiguous. As he puts it, "the uncertainty and ambivalence of professional knowledge may be the subtle secret of its success".[26] Kennedy's view of experts is inspired by other critical analyses claiming that international human rights law is inherently indeterminate, eternally switching between theoretical wrangling and ad hoc application.[27] There is thus good reason to think that experts in international politics outside cybersecurity create ambiguity due to internal competition, outside pressures, and the practical nature of knowledge production.

Critical security studies have used similar theoretical perspectives on practice and performance to problematise the idea of the security 'expert' itself. In this view, security experts use their epistemic capital to promote *insecurity* as much as security, with uncertain moral commitments.[28] Firm distinctions between public and private actors, and between questions of external and internal security, are replaced by what Bigo terms a 'Mobius strip' of professional practices, which creates a dense lattice of relationships between governments and private companies.[29] This symbiotic relationship is explored throughout the empirical chapters of this thesis.

---

[24] Leonard Seabrooke, 'Epistemic Arbitrage: Transnational Professional Knowledge in Action', *Journal of Professions and Organization* 1, no. 1 (1 March 2014): 49–64.
[25] David Kennedy, *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy* (Princeton University Press, 2016), p.278.
[26] Kennedy, p.10.
[27] Martti Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (New York: Cambridge University Press, 2006).
[28] Didier Bigo, 'Security and Immigration: Toward a Critique of the Governmentality of Unease', *Alternatives* 27, no. 1 (1 February 2002): 63–92.
[29] Didier Bigo, 'Globalized (in)Security: The Field and the Ban-Opticon', in *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, ed. Didier Bigo and Anastassia Tsoukala (London; New York: Routledge, 2008), p.39.

Security expertise is ambiguous partly because it centres on the concept of risk. Many social and critical theorists have argued that risk acts as an ur-concept for modernity,[30] forever expanding to new problems, possibilities and calculations.[31] This body of work suggests that risks are not objectively 'there', but that possibilities become risks based on wider political dynamics, and risk calculations can be deployed strategically.[32] Furthermore, risk priorities betray the underlying value structure of society.[33] Calculating risks is, in other words, a way of projecting values into the future.[34] Consequently, questions of threat and risk in security issues are not merely technical, but instead integrate values and facts through expert performance. The ambiguity of expertise identified by Kennedy, then, is amplified for security expertise trading in the currency of risk.

The unclear content of specifically *cybersecurity* expertise has also been noted by several scholars. Stevens has proposed the analysis of cybersecurity expertise in terms of epistemic communities.[35] Quigley *et al* describe the role of cybersecurity experts as that of a "cyber-guru",[36] who simplifies and overstates risks to maximise cybersecurity 'hype'.[37] In contrast, others have followed Kennedy's analysis in arguing that a nuanced and complex expression of risk can be more effective than exaggeration. For example, Zajko suggests that "cybersecurity's expansion has taken place through technocratic developments which often go unremarked in public discussions and political discourse".[38] Barnard-Wills and Ashenden summarise these developments as follows:

[30] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE, 1992).
[31] Jonas Hagmann and Myriam Dunn Cavelty, 'National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity', *Security Dialogue* 43, no. 1 (1 February 2012): 79–96; Karen Lund Petersen, 'Risk Analysis – A Field within Security Studies?', *European Journal of International Relations* 18, no. 4 (1 December 2012): 693–717; Michael Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (London: Demos, 2004).
[32] Claudia Aradau and Rens Van Munster, 'Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future', *European Journal of International Relations* 13, no. 1 (1 March 2007): 89–115.
[33] Mary Douglas, 'Risk as a Forensic Resource', *Daedalus* 119, no. 4 (1990): 1–16.
[34] Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013); Louise Amoore, 'Security and the Incalculable', *Security Dialogue* 45, no. 5 (1 October 2014): 423–39.
[35] Tim Stevens, 'Norms, Epistemic Communities and the Global Cyber Security Assemblage', *E-International Relations* (blog), 27 March 2012, https://perma.cc/8TXC-7XA7.
[36] Kevin Quigley, Calvin Burns, and Kristen Stallard, '"Cyber Gurus": A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection', *Government Information Quarterly* 32, no. 2 (April 2015): 108–17.
[37] Robert M. Lee and Thomas Rid, 'OMG Cyber!', *The RUSI Journal* 159, no. 5 (3 September 2014): 4–12.
[38] Mike Zajko, 'Canada's Cyber Security and the Changing Threat Landscape', *Critical Studies on Security* 3, no. 2 (4 May 2015), p.147.

> It is possible to identify a relatively consistent discourse of cyber security that involves trends of uncertainty, risk perception, securitisation, and potential militarisation. This discourse has complex roots in military, technological, and policy discourses, but its features are not deterministically derived from these, rather occurring at their point of interaction. What has emerged is a techno-political discourse of cyber security… as ungovernable, unknowable, problematically visible, vulnerable, inevitably threatening, and inhabited by a range of hostile and threatening actors.[39]

The combination of 'complex roots' and other 'non-deterministically derived' features mean that cybersecurity has its own vocabulary and mode of performance, rather than being a pure 'colonisation' of cyberspace by military and national security logics.[40] Crucially, the content of the professional cybersecurity discourse, on this view, is fundamentally ambiguous. As Hansen and Nissenbaum observe, "cybersecurity 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".[41] The cybersecurity expert discourse accelerates wider trends to dissolve boundaries between 'types' or 'domains' of security.[42] In his analysis of cybersecurity discourse, Cornish suggests that these trends could be helpful for policymakers, claiming that cybersecurity contains "constructive ambiguity".[43] I modify this characterisation slightly to avoid potentially unwarranted positive connotations, and claim only that the ambiguous professional discourse is *productive*, rather than constructive.

A final source of ambiguity is the foundational role of material and digital objects in constructing cybersecurity expertise. In IR more widely, this insight has been called 'new materialism' or 'new constructivism'.[44] This theoretical perspective rejects an analytical split between the ideational and material, which has a powerful attraction in IR and in the social sciences

---

[39] David Barnard-Wills and Debi Ashenden, 'Securing Virtual Space Cyber War, Cyber Terror, and Risk', *Space and Culture* 15, no. 2 (1 May 2012), pp.110–11.
[40] Mary McEvoy Manjikian, 'From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik', *International Studies Quarterly* 54, no. 2 (1 June 2010): 381–401.
[41] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53, no. 4 (1 December 2009), p.1161.
[42] Rita Abrahamsen and Michael C. Williams, *Security Beyond the State: Private Security in International Politics* (Cambridge; New York: Cambridge University Press, 2010).
[43] Paul Cornish, 'Governing Cyberspace through Constructive Ambiguity', *Survival* 57, no. 3 (4 May 2015): 153–76.
[44] David McCourt, 'Practice Theory and Relationism as the New Constructivism', *International Studies Quarterly* 60, no. 3 (2016): 475–85.

generally.[45] Instead, the technical and social aspects of knowledge production are intertwined: the term 'affordance' prioritizes the former, and 'construction' the latter.[46] This perspective challenges traditional sociological concepts of agency, which are usually granted only to individuals and their composites.[47]

This perspective has significant implications for cybersecurity, especially as the digital objects with which cybersecurity is concerned – such as the Shamoon 'destructive' malware or the Finfisher spyware which began the thesis introduction – are neither clearly material nor ideational. Some scholars have used the hybridity of hardware/software combinations to argue that internet governance, including cybersecurity, should be understood as an interplay between 'code' in both digital and legal forms.[48] Dunn Cavelty and Balzacq have embraced this perspective more comprehensively, suggesting that even "the different spaces created by malware have implications for the way we conceptualise cybersecurity".[49] More specifically, when new malware is discovered, "otherwise stable cybersecurity practices become (temporarily) fluid, thereby making previous order un-orderly, challenging previous knowledge and often exposing previous solutions and assumptions as inadequate."[50]

This fluidity is a key source of uncertainty and ambiguity in the professional discourse. Although this discourse combines both technical and value claims, the latter should not be misinterpreted as purely ideational. Instead, values are concrete things, embodied literally in people,

---

[45] Aihwa Ong and Stephen J Collier, eds., *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems* (Malden, MA: Wiley-Blackwell, 2004); Manuel DeLanda, *A New Philosophy of Society: Assemblage Theory and Social Complexity* (London; New York: Continuum-3PL, 2006); M. Acuto and S. Curtis, eds., *Reassembling International Theory: Assemblage Thinking and International Relations* (Springer, 2013).

[46] For definitions of each, see respectively Samar Faraj and Bijan Azad, 'The Materiality of Technology: An Affordance Perspective', in *Materiality and Organizing: Social Interaction in a Technological World*, ed. Paul Leonardi, Bonnie A. Nardi, and Jannis Kallinikos (Oxford: Oxford University Press, 2013); Ian Hacking, *The Social Construction of What?* (Cambridge, MA: Harvard University Press, 2000).

[47] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford; New York: Oxford University Press, USA, 2007); Andrew Barry, 'The Translation Zone: Between Actor-Network Theory and International Relations', *Millennium - Journal of International Studies* 41, no.3 (1 June 2013): 413–29; Daniel H. Nexon and Vincent Pouliot, '"Things of Networks": Situating ANT in International Relations', *International Political Sociology* 7, no.3 (1 September 2013): 342–45.

[48] Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006).

[49] Thierry Balzacq and Myriam Dunn Cavelty, 'A Theory of Actor-Network for Cyber-Security', *European Journal of International Security* 1, no.2 (July 2016), p.3.

[50] Balzacq and Cavelty, p.15.

software, and organisations. Conversely, strategies, identities and other constituent elements of IR actors are simultaneously material, technological and conceptual. My understanding of knowledge production in cybersecurity is thus indebted to the theoretical traditions of new materialism and new constructivism.

However, the analytical framework taken by this thesis provides an important corrective to such accounts. As Waelbers and Dorstewitz have argued, "although [this] approach is rich in that it enables scholars to interrelate many complex factors in their studies, the approach is poor from an ethical perspective" because "the doings of people are viewed merely as functions within a technological environment".[51] In other words, it has a very thin understanding of morality. Instead, they suggest, "moral agency [should be] seen as embedded within an environment, to which it adapts and within which it evolves."[52] This thesis takes the ambiguity of cybersecurity professional discourse as a starting point from which to examine precisely this embedded moral agency within the cybersecurity expert community. It does so by using the original concept of moral manoeuvres, to which I now turn.

2.2 Moral manoeuvres

This section argues that the concept of moral manoeuvres – defined as the alteration of technical and value claims in an expert discourse and the renegotiation of the relationship between them – provides a better explanation of the nature of cybersecurity in Egypt and the Gulf states than the two closest alternatives, based on securitisation theory and norm studies.

[51] Katinka Waelbers and Philipp Dorstewitz, 'Ethics in Actor Networks, or: What Latour Could Learn from Darwin and Dewey', *Science and Engineering Ethics* 20, no. 1 (March 2014), p.24.
[52] Waelbers and Dorstewitz, p.38.

2.2.1 Cyber securitisation

One of the key insights of critical security studies, as a subfield of IR, is that conceptions of threat and vulnerability are not natural or universal.[53] This insight extends earlier analyses claiming to dissect purely conceptual distinctions in the concept of security.[54] Seminal works in critical security studies have built on this insight to problematise the idea of security itself, showing that issues are not matters of security *intrinsically* but become so through processes of 'securitisation'.[55] Securitisation, in its original version, suggested that security is the discursive result of a speech act, a linguistic performance that 'speaks security' rather than an immutable aspect of the international system. This performance involves the construction of both something that needs to be secured (a 'referent object') and a threat to that referent object.[56] The effects of securitisation include extra resources and the prevention of challenge, moving issues out of the terrain of normal politics.[57] Securitisation has echoes in the broader concept of 'framing' as a means of influencing politics,[58] and has the emancipatory aim of reframing security issues in a different light ('de-securitisation').

Many cybersecurity scholars have used securitisation theory to demonstrate that cybersecurity is constructed by actors speaking 'cybersecurity' to an audience in a particular context.[59] This construction is a combination of both technical claims about the properties of

[53] Keith Krause and Michael C. Williams, eds., *Critical Security Studies: Concepts And Strategies* (London: Routledge, 1997); Richard Wyn Jones, *Security, Strategy and Critical Theory* (Boulder, Colo: Lynne Rienner Publishers, 1999); Ken Booth, ed., *Critical Security Studies and World Politics* (Boulder, Colo: Lynne Rienner Publishers, 2004).

[54] Arnold Wolfers, '"National Security" as an Ambiguous Symbol', *Political Science Quarterly* 67, no. 4 (1952): 481–502; David A. Baldwin, 'The Concept of Security', *Review of International Studies* 23, no. 1 (January 1997): 5–26.

[55] Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, Colo: Lynne Rienner Publishers, 1997); Thierry Balzacq, ed., *Securitization Theory* (Oxford; New York: Routledge, 2010); Michael C. Williams, 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly* 47, no. 4 (1 December 2003): 511–31; Ole Wæver, 'Politics, Security, Theory', *Security Dialogue* 42, no. 4–5 (1 August 2011): 465–80; Jef Huysmans, 'Security! What Do You Mean?: From Concept to Thick Signifier', *European Journal of International Relations* 4, no. 2 (1 June 1998): 226–55.

[56] Buzan, Waever, and Wilde, *Security*.

[57] This aspect of securitisation theory has changed significantly: for an overview, see Wæver, 'Politics, Security, Theory'. It should be noted that 'securitisation' has acquired a wider meaning of the prioritization of security over other goals or rights, which stems from but is not identical to securitisation theory in IR.

[58] Scott D. Watson, '"Framing" the Copenhagen School: Integrating the Literature on Threat Construction', *Millennium* 40, no. 2 (1 January 2012): 279–301.

[59] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics* (London, New York: Routledge, 2008); Barnard-Wills and Ashenden, 'Securing Virtual Space Cyber War, Cyber Terror, and Risk'; Zajko, 'Canada's Cyber Security and the Changing Threat Landscape'; Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics

computers and digital networks, and implicit values contained in claims about risks surrounding such networks. One influential intervention summarised this combination by stating simply that "cyber security can be seen as 'computer security' plus 'securitisation'".[60] The high salience of the term cyber*security* in international politics indicates that it is - almost by definition - a successful securitisation.

Despite this success, I argued above that the referent object for cybersecurity professional discourse remains ambiguous. Cybersecurity therefore cannot only be understood as the construction of a clear referent object that needs to be secured, as classical securitisation theory suggests. We need to move beyond binary views of successful or failed securitisation to explore how, even *within* a successfully securitised issue, there remains a fundamental ambiguity about what security experts seek to protect, and how this ambiguity affects the behaviours, strategies and identities of cybersecurity actors. This is the purpose of the concept of moral manoeuvres, which has much in common with the process of securitisation, although it is more closely related to the 'Paris' school, focusing on expert practices, rather than the 'Copenhagen' school, focusing on speech acts.[61] However, in contrast to securitisation, it takes the ambiguity of professional discourse as its starting point, rather than seeing ambiguity as a problematic or incomplete aspect of cyber securitisation.

Some critical cybersecurity scholars acknowledge that cybersecurity is the site of a range of securitising moves. For example, Dunn Cavelty and Jaeger have argued that the hacker collective 'Anonymous' (which will feature in Chapter 5) articulates what they call a 'counter-securitisation' as well as embracing the 'Othered' identity it has in mainstream cybersecurity. In a passage worth quoting at length, they argue:

> Anonymous does not just passively emerge as a threat by state designation, but is actively taking part in its own securitisation by forcefully undercutting the state's prerogative to secrecy and authoritative information. Moreover, it also suggests and successfully establishes counter-securitisations, in which the state is presented as the main threat. Therefore, this political conflict is itself characterised, fueled, and sustained

in US Critical Infrastructure Protection', *Information&Security* 7 (2001): 80–103; Johan Eriksson and Giampiero Giacomello, *International Relations and Security in the Digital Age* (Routledge, 2007); Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School'.

[60] Hansen and Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', p.1160.

[61] C.A.S.E. Collective, 'Critical Approaches to Security in Europe: A Networked Manifesto', *Security Dialogue* 37, no. 4 (1 December 2006): 443–87.

> by conflicting meaning-making, in which a process of reciprocal securitisation is serving a complex and curious identity function on both sides of the social conflict.[62]

This passage highlights the ambiguity central to cybersecurity professional discourse, characterising it as the result of a 'process of reciprocal securitisation'. While this accurately identifies some of the dynamics explored by this thesis, Dunn Cavelty and Jaeger's analysis is limited by their theoretical apparatus for describing these dynamics, with a choice between either securitisation or counter-securitisation. In contrast, the alteration and renegotiation of values and technical claims in cybersecurity is not necessarily 'reciprocal' or opposed, but instead occurs multidimensionally, with actors using the ambiguous expert discourse to pull cybersecurity in multiple directions.

The concept of moral manoeuvres captures this phenomenon, extending the work of critical security studies by showing how security domains, despite their foundational constructions of threat and victim, accommodate a wide range of values that are constantly contested and redefined in light of specialised technical claims. Overall, security is full of a rich variety of moral judgements and relations, as classical realism recognised more explicitly than later versions.[63] The concept of moral manoeuvres thus complements Dunn Cavelty and Jaeger's sophisticated analysis by providing a rigorous analytical framework in which the 'conflicting meaning-making' of various cybersecurity actors can be placed.

Another way of specifying the contribution of this thesis to critical security studies is by saying that the concept of moral manoeuvres is both narrower and wider than the concept of securitisation. It is narrower in the sense that moral manoeuvres can take place *within* security issues, rather than adopting a wide-angle view of securitisation as a binary process where issues are either securitised or not, and securitisations are 'successful' or 'failed'.[64] On the other hand, the concept of moral

[62] Myriam Dunn Cavelty and Mark Daniel Jaeger, '(In)Visible Ghosts in the Machine and the Powers That Bind: The Relational Securitization of Anonymous', *International Political Sociology* 9, no. 2 (1 June 2015), p.177.
[63] Jim George, 'Realist "Ethics", International Relations, and Post-Modernism: Thinking Beyond the Egoism-Anarchy Thematic', *Millennium* 24, no. 2 (1 July 1995): 195–223.
[64] Juha A. Vuori, 'A Timely Prophet? The Doomsday Clock as a Visualization of Securitization Moves with a Global Referent Object', *Security Dialogue* 41, no. 3 (1 June 2010): 255–77.

manoeuvres is wider than securitisation because moral manoeuvres – the reinterpretation of values in an issue area - can also happen outside security contexts. The concept of moral manoeuvres goes beyond a pure polarisation of what securitisation theory calls 'normal politics' and provides a more nuanced theoretical framework for understanding interaction within this issue area.

Finally, understanding cybersecurity as formed through several distinct moral manoeuvres provides a solution to what Dunn Cavelty elsewhere calls the 'cybersecurity dilemma': namely, that "we cannot have both a strategically exploitable cyberspace full of vulnerabilities and a secure and resilient cyberspace that all the cybersecurity policies call for".[65] To understand how this dilemma arises, we need to ask how disparate values in cybersecurity legitimate this apparently contradictory outcome. This thesis suggests that the cybersecurity dilemma emerges from several separate moral manoeuvres, each exploiting the ambiguity of cybersecurity professional discourse to define cybersecurity differently. It is these moral manoeuvres that create Dunn Cavelty's cybersecurity dilemma, and dissolving it requires us to first understand the moral manoeuvres themselves.

2.2.2 Cyber norms

Another closely related approach to values in cybersecurity is work on 'cyber norms', which draws on a different set of critical and constructivist literature. This section argues that the concept of moral manoeuvres provides a better explanation of the nature of cybersecurity in Egypt and the Gulf states than this literature, as well as the contribution to the cyber securitisation literature above.

Norms have been paradigmatically defined in IR as "standards of appropriate behaviour for actors with a given identity" in the international sphere.[66] Through such definitions, the norms literature avoids specific ideas about which things to value in theory, even if it imports such assumptions in practice.[67] Norm theories also do not restrict value judgements to cases where overtly

[65] Myriam Dunn Cavelty, 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', *Science and Engineering Ethics*, 2014, p.711.
[66] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* 52, no. 4 (1998), p.891.
[67] Margaret E. Keck and Kathryn Sikkink, *Activists beyond Borders: Advocacy Networks in International Politics* (Ithaca: Cornell University Press, 1998); Thomas Risse-Kappen, Stephen C. Ropp, and Kathryn

moral language is used; norms can take any form and be expressed in any language.[68] Many scholars have emphasised that international security is as apt an environment for norms as any other domain of politics.[69] As Hurrell suggests, questions of security cannot be considered in isolation from the wider moral environment in which they arise, because "the normative ambition of international society in relation to security… has been driven in part by moral concerns".[70] Norm theories also include expert discourses as a key aspect of value-based dynamics in international politics: the early norms literature considered epistemic communities to be central to the activity of transnational advocacy networks, and later theories of norm contestation also see epistemic communities as a key site of contest.[71]

Cybersecurity studies in IR have drawn on the norms literature since their inception. For example, in their original exposition of the concept of 'netwar', Arquilla and Ronfeldt used Keck and Sikkink's work to argue that the internet would assist and amplify the efforts of transnational advocacy networks.[72] Other scholars have called for the development of norms in relation to cyber conflict and cyber rights.[73] Unsurprisingly, norm studies has been used to analyse not just cybersecurity, but also internet governance more widely. Raymond has argued that the prospects for norms in internet governance depend on whether the internet is viewed as a vehicle for sovereign

---

Sikkink, *The Power of Human Rights: International Norms and Domestic Change* (Cambridge University Press, 1999); Beth A. Simmons, *Mobilizing for Human Rights: International Law in Domestic Politics* (Cambridge; New York: Cambridge University Press, 2011); Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink, *The Persistent Power of Human Rights: From Commitment to Compliance* (Cambridge: Cambridge University Press, 2013).

[68] Mervyn Frost, *Ethics in International Relations: A Constitutive Theory* (Cambridge; New York: Cambridge University Press, 2008), pp.100-102; Friedrich V. Kratochwil, *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs* (Cambridge: Cambridge University Press, 1991), pp.69-94; Richard M. Price, ed., *Moral Limit and Possibility in World Politics* (Cambridge; New York: Cambridge University Press, 2008), pp.3-6.

[69] Richard Price, 'A Genealogy of the Chemical Weapons Taboo', *International Organization* 49, no. 1 (1995): 73–103; Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945* (Cambridge: Cambridge University Press, 2007); Jennifer M. Welsh, 'Norm Contestation and the Responsibility to Protect', *Global Responsibility to Protect* 5, no. 4 (1 January 2013): 365–96.

[70] Andrew Hurrell, *On Global Order: Power, Values, and the Constitution of International Society* (Oxford; New York: Oxford University Press, 2008), p.191.

[71] Keck and Sikkink, *Activists beyond Borders*; Antje Wiener, *A Theory of Contestation* (New York: Springer, 2014).

[72] John Arquilla and David Ronfeldt, 'The Advent of Netwar: Analytic Background', *Studies in Conflict & Terrorism* 22, no. 3 (1 August 1999), p.202.

[73] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015); Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012); Chelsey Slack, 'Wired yet Disconnected: The Governance of International Cyber Relations', *Global Policy* 7, no. 1 (1 February 2016): 69–78.

power or as a global commons.[74] I will return to broader debates over cyber sovereignty and its alternative, an open 'multistakeholder' internet, in Chapter 3.

There are four main texts commonly cited as norms in cybersecurity. In chronological order, the first is the Budapest Convention on Cyber Crime, agreed by the Council of Europe in 2001.[75] The second is the Tallinn Manual on the conduct of military cyber operations, first published by NATO in 2012.[76] The third is the amendment of the Wassenaar Arrangement, an arms control agreement, in 2013 to include surveillance technologies as dual-use controlled exports.[77] The fourth is the agreement of the UN Group of Governmental Experts (GGE) on cybersecurity in 2015 that the Laws of Armed Conflict apply to cyberwarfare (although the group itself had been meeting for much longer).[78] Other norm candidates come from the private sector, especially Microsoft's controversial Digital Geneva Convention, which calls for transparency over state actions and greater protection for non-state actors.[79] Bilateral state agreements are sometimes mentioned; for example, there was a high profile US-China agreement to prevent cybercrime in 2015.[80] These norms have been recognised by scholars outside critical or constructivist approaches; for example, Nye includes 'normative deterrence' as a key element of US cyber strategy.[81]

However, these cyber norms have all been criticised for two reasons: first, their exploitation and strategic use; and second, their lack of normative power due to disagreements over underlying values. I consider these problems in turn.

---

[74] Mark Raymond, 'Puncturing the Myth of the Internet as a Commons', *Georgetown Journal of International Affairs*, no. Special Issue (2013): 5–15.
[75] Council of Europe, 'Convention on Cybercrime (the Budapest Convention)' (European Treaty Series - No.185, 23 November 2001).
[76] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge England ; New York: NATO CCDCOE, Cambridge University Press, 2013).
[77] Colin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies' (Access, 2015).
[78] Levi Maxey, 'Can the Law Restrain Nations in Cyberspace?', *The Cipher Brief* (blog), 6 August 2017, https://perma.cc/WB8F-WFUA.
[79] Brad Smith, 'The Need for a Digital Geneva Convention', *Microsoft on the Issues* (blog), 14 February 2017, https://perma.cc/LTR3-ESKL.
[80] Catherine Laporte-Oshiro and James Shires, 'Negotiating Order in Cyberspace: Security Spirals or Trade Foundations?' (German Marshall Fund, Brussels, February 2016).
[81] Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (1 January 2017): 44–71.

Cybersecurity norms are problematic most simply because they are regarded as one-sided and promoted for strategic advantage. For example, Hurwitz argues that the Tallinn Manual authors "have been criticised *ad hominem* for their associations with NATO", implying that critics see the Tallinn Manual as biased towards 'Western' views of cybersecurity.[82] The GGE process and its collapse has been extensively analysed by cybersecurity scholars in these terms. Tikk-Ringas has claimed that the GGE statements "make use of norms as an instrument of power", concluding that cyber norms "target the current balance of power and speak to diverging visions of what ought to be. Norms, as technology itself, serve calculated and purposeful aspirations".[83] Similarly, in an article starkly titled "The end of cyber norms", Grigsby argues that the fundamental problem with the 5th GGE report in 2015 was that "Western countries saw norms as a vehicle through which they could improve the stability of cyberspace by establishing a series of easily digestible rules based on existing international law". However, this was interpreted by Russia and China as "trying to find justifications in international law for the use of cyber means during a conflict or of conventional means as a way to respond to cyber conflict."[84] The collapse of the GGE process in 2017 reflected the failure of this Western vision, and underlined the consequences of the strategic promotion of particular cyber norms.

The second problem with cyber norms is that they conceal deep differences in underlying values. In 2011 and 2012, a series of workshops on cyber norms held across several US universities concluded that cyber norms were limited by disagreement in "core political values".[85] Erskine and Carr highlight these disagreements, arguing that cyber norms conceal "the tensions and even blatant contradictions between the various value systems that these globalised practices bring together".[86] They warn that "an eventual convergence of values cannot be assumed… Understanding norms in

[82] Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace', *American Foreign Policy Interests* 36, no. 5 (3 September 2014), p.328.
[83] Eneken Tikk-Ringas, 'International Cyber Norms Dialogue as an Exercise of Normative Power', *Georgetown Journal of International Affairs* 17, no. 3 (2017), p.47.
[84] Alex Grigsby, 'The End of Cyber Norms', *Survival* 59, no. 6 (2 November 2017), pp.111, 113.
[85] Participants, 'A Call to Cyber Norms: Discussions at Workshops, 2011 and 2012' (Harvard-MIT-University of Toronto, 2013), https://perma.cc/J884-EKXE, p.42.
[86] 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 (NATO CCDCOE, 2016), p.96.

cyberspace demands attention to the complexities of their underlying values".[87] Finnemore and Hollis go further, suggesting that "if multiple actors continually pursue a closer alignment of the norm to their basic goals, values, or interests, we can expect that incompletely theorised norms may become a locus of *constant discord*" (my italics).[88] Finnemore and Hollis go on to encourage their readers to "think holistically" about the "larger fabric of norms", or the "larger norm landscape".[89] I take their suggestion seriously, as I draw on not only a 'fabric of norms' but also a wider canvas of clustered values to provide a rigorous account of how constant discord is a fundamental aspect of cybersecurity.

The concept of moral manoeuvres addresses both problems with cyber norms. First, moral manoeuvres are a way of describing the reinterpretation of values and technical claims without requiring a clear norm as the focal point. This concept enables us to analyse how actors negotiate the whole 'dense normative web' of an issue like cybersecurity rather than specific norms *within* those issues. Although the cyber norms of the Budapest Convention and the Wassenaar Arrangement appear regularly in the empirical body of the thesis, in each case I show that these norms are only one part of a broader moral manoeuvre. Second, moral manoeuvres are not just aimed at achieving specific goals, but also change the issue area of cybersecurity overall. The shifting reproduction of issue areas is often underplayed by cyber norm scholars in order to focus on the effect of rules over time; in contrast, the argument here emphasises that moral manoeuvres redefine cybersecurity itself.

I now consider two objections to the concept of moral manoeuvres rather than an analysis in terms of cyber norms: first, that the concept of norm itself can be extended to include moral manoeuvres, and second, that this is an expected part of the early stage of a norm 'lifecycle'.

First, norms are much more varied than suggested by their portrayal in 'first-generation' norm studies.[90] This has led scholars to argue that the meaning of norms is defined continually

[87] Erskine and Carr, p.97.
[88] Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International Law* 110, no. 3 (July 2016), p.473.
[89] Finnemore and Hollis, pp.464, 477.
[90] E.g. Audie Klotz, *Norms in International Relations: Struggle Against Apartheid* (Ithaca: Cornell University Press, 2000).

through use, or that norms are processes rather than rules.[91] Others have built flexibility into international norms through specific processes of localisation, translation and contestation.[92] In some treatments, the concept of norm itself has been stretched almost to breaking point; for example, one definition suggests that norms are no more than "the weighted valuing of the wide range of things people do".[93] These developments in the norms literature suggest that the alteration of and renegotiation between values and technical concepts investigated by this thesis could be conducted in terms of norms without introducing the concept of moral manoeuvres.

However, these sophisticated treatments of norms all exhibit the same tension: namely, that the more the possibility for reinterpreting a norm is emphasised, the less coherent or norm-like the norm itself becomes. In cybersecurity, this tension is apparent in the work of Finnemore and Hollis cited above, whose explicit aim is 'constructing norms for global cybersecurity'. Their article applies the latest developments in norm studies to cybersecurity, including ideas of contest, process, and localisation, as follows:

> Every time actors follow a norm, they interpret it… Each interpretation, each episode of conformity with a norm (or failure to conform) accretes... When the norm context is as varied as cybersecurity, every application of a norm is a bit different, adding rich layers of shared understanding over time about the lines of acceptable behaviour in different circumstances... Because of the repeated application and interpretation of norms, not only do norms shape the behaviour of actors with a given identity, but the actions of those actors shape, in turn, the contours and content of norms.[94]

My understanding of normative dynamics is indebted to this work. However, its metaphor is misleading. If 'every application of a norm is a bit different', layers of experience do not necessarily accrete into a 'shared understanding' in the way that sedimentary rock piles strata upon strata, cementing the norm in the process. It is equally possible that new applications fracture and dissolve

[91] Mona Lena Krook and Jacqui True, 'Rethinking the Life Cycles of International Norms: The United Nations and the Global Promotion of Gender Equality', *European Journal of International Relations* 18, no. 1 (1 March 2012): 103–27; Susanne Zwingel, 'How Do Norms Travel? Theorizing International Women's Rights in Transnational Perspective', *International Studies Quarterly* 56, no. 1 (1 March 2012): 115–29.
[92] Amitav Acharya, 'How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism', *International Organization* 58, no. 2 (2004): 239–75; Lisbeth Zimmermann, *Global Norms with a Local Face: Rule-of-Law Promotion and Norm Translation* (Cambridge, UK; New York: Cambridge University Press, 2017); Wiener, *A Theory of Contestation*.
[93] Christopher Kutz, 'How Norms Die: Torture and Assassination in American Security Policy', *Ethics & International Affairs* 28, no. 4 (2014), p.427.
[94] Finnemore and Hollis, 'Constructing Norms for Global Cybersecurity', p.453.

previous actions, questioning and undermining the foundations of shared understanding that were previously taken for granted. This has been ably demonstrated by Stevens, who initially claimed that cyber norms, as part of an "emerging global governance architecture", were developing "quietly and haltingly".[95] However, he later argued instead that prevailing forms of power had created a 'nonregime' in cybersecurity,[96] moving beyond fragmentation to the deliberate absence of what Finnemore and Hollis call 'lines of acceptable behaviour' in the quotation above. The difference between an approach in terms of cyber norms and one in terms of moral manoeuvres is that cyber norms presume eventual cohesion, whereas moral manoeuvres can equally preserve or increase existing ambiguities and contradictions. In other words, there is an ongoing gaming of the value structure of cybersecurity, involving moves in several directions rather than either progress and retrogression or direct opposition and contest.

The second objection is that cybersecurity norms are merely at an early stage in their 'life-cycle', in the model proposed by Keck and Sikkink and expanded by Sandholtz and Stiles.[97] In this view, the nascent state of the issue itself excuses a lack of normative cohesion, as cyber norms have yet to become truly 'settled'. There is an understandable policy-linked obligation, especially in the US, to espouse norm theory as an analytically coherent approach to cybersecurity and to explain the problems above by emphasising the 'novelty' of cybersecurity as the chief reason for the lack of clear cybersecurity norms. For example, the US workshops on cyber norms cited above concluded that "existing cyber norms seem inadequate or insufficiently clear and accepted to constrain these activities… Arguably, new norms are needed to specify the rights, responsibilities, and prohibitions for states and other actors in cyberspace."[98]

However, this route is perhaps too easy a way out. As Stevens notes in his comprehensive treatment of the politics of time in cybersecurity, the narrative of novelty for cybersecurity is

[95] Tim Stevens, 'Cyberweapons: An Emerging Global Governance Architecture', *Palgrave Communications* 3, no. 16102 (10 January 2017), p.5.
[96] Tim Stevens, 'Cyberweapons: Power and the Governance of the Invisible', *International Politics* 55, no. 3 (1 May 2018): 482–502.
[97] Wayne Sandholtz and Kendall Stiles, *International Norms and Cycles of Change* (Oxford; New York: Oxford University Press, 2008).
[98] Participants, 'A Call to Cyber Norms: Discussions at Workshops, 2011 and 2012', p.1.

deceptively simple. Novelty is not an external condition to which cybersecurity experts must respond, but rather a concept of time integral to the field itself. As he observes, "the field of cyber security seems pervaded by a profound sense of frustration and disorientation at being trapped in an accelerating present, cut off by history".[99] In other words, continued claims of novelty can mask underlying dynamics preventing cyber norms from ever progressing through their life-cycle – which nearly all norms scholars recognise is not inevitable - and shield cyber norms from a clear appraisal of their development so far. Whatever the future of cyber norms and the policy requirements for their support, the policy task is different to the analytical one undertaken in this thesis: to provide a theoretically grounded and empirically defensible account of actual moral interaction.

Overall, the language of norms - unless stretched beyond what good faith would permit - is insufficient to adequately capture the value relationships at work in cybersecurity. Although one could extend norms to meet this challenge, it may be more fruitful to describe this phenomenon in other terms. This shift in focus enables an analysis of value-based dynamics in cybersecurity that avoids diluting the concept of norm beyond theoretical utility. We can therefore extend Cornish's conclusion that "it would surely be feasible to concede that there might not, after all, be such a thing as a 'normal state' (usually meaning one in the Western mould) to which other governments and societies should seek to conform" by providing a robust theoretical alternative.[100] Instead of a normal state, we have moral manoeuvres performed simultaneously by actors with various motivations, creating a tapestry of actions woven intricately together with much tension in the constituent threads. The key question is how to distinguish these moral manoeuvres, to which I now turn.

2.3 Invested and agnostic actors

The third key claim of this thesis is that we can identify four different moral manoeuvres based on the motivation of the actors involved, as either *invested* or *agnostic*. Invested actors seek to promote a particular value or cluster of values in an issue area, while agnostic actors seek a

[99] Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge: Cambridge University Press, 2015), p.93.
[100] Cornish, 'Governing Cyberspace through Constructive Ambiguity', p.171.

separate goal (in this case, economic) without preference for a particular value or cluster of values. In this section, I first argue that this distinction cuts across existing IR understandings of interests and power. I then show how the four moral manoeuvres derived from this distinction – alignment, appropriation, manipulation, and elision – are an important complement to specific norm-based alternatives.

2.3.1 Interests and power

IR works often employ a distinction between normative action, performed for value-based reasons, and strategic action, performed for self-interest.[101] Both critical and constructivist scholars have noted an overlap between these two motivations in cybersecurity. From a critical perspective, Deibert argued in a prescient chapter in 2002 that "the internet security problematic is not a unified field but a complex intersection of interests and values, some of which overlap and some of which collide."[102] Similarly, Simon and de Goede used similar language to that employed in this thesis to analyse what they call "the banal bureaucratic manoeuvres" in EU cybersecurity.[103]

From a constructivist perspective, several scholars have also highlighted the overlap between interests and values. Carr has argued that although there is "an aspiration to promote liberal norms and values" in US internet policies, there is also "the acknowledgement of the reality that some limits on this right [to Internet freedom] can best promote and protect US interests".[104] Powers and Jablonski, in their treatment of the same issues (which they call 'the real cyberwar'), identify a "prevailing narrative equating the U.S. doctrine of internet freedom with a virtuous defense of freedom of expression", which they contrast with "the underlying economic and geo-strategic

[101] A classic critique is Finnemore and Sikkink, 'International Norm Dynamics and Political Change', p.888.
[102] Ronald J. Deibert, 'Circuits of Power: Security in the Internet Environment', in *Information Technologies and Global Politics*, ed. James N. Rosenau and J. P. Singh (Albany, NY: State University of New York Press, 2002), p.117.
[103] Stephanie Simon and Marieke de Goede, 'Cybersecurity, Bureaucratic Vitalism and European Emergency', *Theory, Culture & Society* 32, no.2 (1 March 2015), p.82.
[104] Madeline Carr, 'Internet Freedom, Human Rights and Power', *Australian Journal of International Affairs* 67, no. 5 (1 November 2013), p.626.

motivations driving U.S. information policy."[105] In cybersecurity, then, it is difficult to disentangle interested and normative motivations.

More generally, the problem with the distinction between interested and normative action is that values can both be objects within a strategic calculation *and* goals that direct the behaviour of actors.[106] Consequently, as Dill suggests, the difference between strategic action for 'interests' and normative action performed 'morally' is not hard and fast.[107] However, whereas Dill retains the interested and normative distinction, separating the two based on their time frame – near-term goals are interests, whereas long-term goals are normative – I instead distinguish actors based on two intermediate categories of action, both of which allow interests and values to mix. *Invested* actors, such as the states and NGOs considered in this thesis, seek to promote a particular value, but can do so for a combination of normative and interested reasons. *Agnostic* actors, such as the international surveillance suppliers and the wider cybersecurity industry, seek to navigate between different values, in this case for economic gain. Some scholars have argued that values are incorporated into profit-based motivations and so even economic action is not purely self-interested.[108]

This view of action makes no claims about inaccessible mental states. Partly, this is useful because such a claim would be metaphorical, given the corporate and organisational actors considered in this thesis. More importantly, this view is based on the intuition that motivations are constructed intersubjectively, rather than signalled by the presence of particular 'internal' processes. Motivation is defined by the actor in a way that is intelligible to their wider community, rather than being a linear relationship between an internal 'desire' and 'belief' and an external action to

[105] Shawn M. Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana: University of Illinois Press, 2015), p.205.
[106] As Dillon and Reid put it, "Liberal strategizers… must necessarily look to control the very process of morphogenesis itself... They are not only interested in asking which forms of life are good, bad or indifferent… they are compelled to ask what kind of living things we might prefer to have, and how they can be formed." Michael Dillon and Julian Reid, *The Liberal Way of War* (London; New York: Routledge, 2009), p.44.
[107] Janina Dill, *Legitimate Targets?: Social Construction, International Law And Us Bombing* (Cambridge, UK: Cambridge University Press, 2014), pp.48-49. Dill acknowledges that this amounts to almost a "sleight of hand".
[108] Malcolm Campbell-Verduyn, *Professional Authority After the Global Financial Crisis: Defending Mammon in Anglo-America* (New York, NY: Palgrave Macmillan, 2017).

efficiently realise that desire. Affect and emotion also play key roles in motivation.[109] Consequently, a distinction between invested and agnostic actors is compatible with several logics of action in IR.[110]

The invested/agnostic distinction has two further benefits, combining several facets of power in international politics.[111] First, the category of invested actors bypasses a tension between critical and constructivist approaches to power. On one hand, constructivist scholars suggest that power can be derived from particular values. Carr observes that "US politicians frequently make reference to US power as *emerging* from… values and principles", suggesting that they "regard US power as contingent upon the political will to adhere to the kind of 'moral framework' which they feel makes that state exceptional."[112] On the other hand, as critical theories suggest, value judgements can be *merely* the expression of power. Bourdieu argued that the value structure of a field was a form of 'symbolic' power, meaning the sublimated expression of hierarchy and domination through apparently cultural or subjective judgement (notwithstanding the many difficulties in the definition of 'symbolic' itself).[113] The category of invested actors is compatible with both these relationships between values and power, as it claims only that invested actors use various forms of power to promote a value or cluster of values, without specifying whether their power is derived from or masquerades as those values.

Second, the category of agnostic actors forms a point of contact between critical approaches to cybersecurity on the one hand and revisions to mainstream approaches made by cybersecurity scholars on the other. From a critical perspective, Deibert has argued that cybersecurity is characterised by multiple "circuits of power":

---

[109] Todd H. Hall, *Emotional Diplomacy: Official Emotion on the International Stage* (Ithaca; London: Cornell University Press, 2015).

[110] James G. March and Johan P. Olsen, 'The Institutional Dynamics of International Political Orders', *International Organization* 52, no. 4 (1998): 943–69; Thomas Risse, '"Let's Argue!": Communicative Action in World Politics', *International Organization* 54, no. 1 (2000): 1–39; Vincent Pouliot, 'The Logic of Practicality: A Theory of Practice of Security Communities', *International Organization* 62, no. 2 (April 2008): 257–88; Ted Hopf, 'The Logic of Habit in International Relations', *European Journal of International Relations* 16, no. 4 (1 December 2010): 539–61; Jérémie Cornut, 'Diplomacy, Agency, and the Logic of Improvisation and Virtuosity in Practice', *European Journal of International Relations* 24, no. 3 (8 September 2017).

[111] Barnett and Duvall, 'Power in International Politics'; Barry Hindess, *Discourses of Power: From Hobbes to Foucault* (Oxford, UK; Cambridge, Mass., USA: John Wiley & Sons, 1996).

[112] Carr, 'Internet Freedom, Human Rights and Power', p.624.

[113] Pierre Bourdieu, *The Logic of Practice* (Cambridge: Polity Press, 1992); Rebecca Adler-Nissen, ed., *Bourdieu in International Relations: Rethinking Key Concepts in IR* (New York: Routledge, 2013).

> As dominant security concerns shift their focus to the network, the nature and exercise of power will be transformed as well. Rather than being associated with the control of territory—a space-of-places, in Castell's words—power will increasingly be manifested in the control over a "space-of-flows". Regulation, direction, and restriction of the tempo and access to circuits of information, in other words, could become the most significant bases of political power.[114]

Deibert has pursued this focus on power as restriction and access to information in academic fora and with Citizen Lab (covered in more detail in Chapter 6).[115] In general, he has promoted the idea of 'black code'; the use of cyberspace for a wide variety of aims unseen by and often deliberately hidden from democratic societies.[116] Much of this black code is produced by 'agnostic' corporate actors, who navigate between value clusters rather than adhering to or promoting any specific values.

The category of agnostic actors is also useful for mainstream IR approaches to power and cybersecurity. Most influentially, Nye has put forward a concept of 'cyberpower', defined as "a set of resources that relates to the creation, control, and communication of electronic and computer-based information".[117] For Nye, cyberpower is part of the overall diffusion of power from states to non-state actors in the international system. Harknett also argues that cyberspace is a domain of constant strategic struggle falling short of war.[118] Like others pushing the boundaries of strategic studies,[119] Harknett stresses that power in cybersecurity permeates deep into politics outside violent conflict, relying on the tactical use of information, media strategies, and private actors, and redefining concepts like sovereignty and national boundaries. Both Harknett and Nye highlight how actors who are not committed to particular values shape the terrain of cybersecurity and of digital

[114] Deibert, 'Circuits of Power: Security in the Internet Environment', p.134.
[115] Ronald J. Deibert, 'Bounding Cyber Power: Escalation and Restraint in Global Cyberspace' (Centre for International Governance Innovation, October 2013); Ronald J. Deibert and Rafal Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4, no. 1 (1 March 2010): 15–32; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War', *Security Dialogue* 43, no. 1 (1 February 2012): 3–24; Ronald J. Deibert, 'Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace' (Canadian Defence and Foreign Affairs Institute, August 2012).
[116] Ronald J. Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium - Journal of International Studies* 32, no. 3 (1 December 2003): 501–30; Ron J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Plattsburgh, NY: Signal Books, 2013).
[117] Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), p.123.
[118] Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61, no. 3 (1 January 2017): 381–93.
[119] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Adelphi Series (Routledge, 2011).

politics more generally. Harknett writes within a very different literature to the critical scholars above, and Nye avoids discussion of what he calls the 'reflexive' analysis of power – i.e. that undertaken by critical security studies - because he finds the insights gained "purchased at too high a price".[120] Nonetheless, the category of agnostic actors, moving between different value clusters and exercising both technical 'cyber' power and a range of other strategies, provides a bridge between these works and more critical approaches.

In sum, the distinction between invested and agnostic actors combines both interested and normative motivations for action in international politics. It avoids claims about specific inner states to highlight an analytically useful understanding of intermediate-level motivations. Both categories also contribute to existing approaches to power in cybersecurity: the category of invested actors bypasses a tension between critical and constructivist views of power and values, while the category of agnostic actors provides a bridge between critical views of power and similar approaches in revisionist strategic studies applied to cybersecurity.

2.3.2 Four moral manoeuvres

The distinction between invested and agnostic actors is the basis for specifying the four moral manoeuvres considered in this thesis, as follows. First, invested actors can seek to reframe their value preferences to fit the existing cybersecurity expert discourse, which I call *alignment*. Second, invested actors can do the opposite and seek to expand the discourse to fit their value preferences, which I call *appropriation*. Third, actors who are agnostic between different values or clusters of values can seek to exploit the contradictions between values within the discourse, which I call *manipulation*. Fourth, agnostic actors could also do the opposite and minimise these contradictions, which I call *elision*. As stated in the introduction, this list does not exhaust the possible space of moral manoeuvres, although it does represent four intuitive ways in which actors can renegotiate technical and value claims.

[120] Nye, *The Future of Power*, p.242 (footnote).

These four moral manoeuvres each have alternative norm-based explanations, as the norms literature has analysed extensively how some actors are particularly influential in norm development, including concepts of norm 'entrepreneurs' and 'antipreneurs'.[121] These actors are often strategic: for example, scholars have identified struggles between groups deploying moral arguments to their advantage in both the 'left' activist networks that are the focus of most norm theory *and* the global right wing.[122] Other scholars have identified the strategic use of rhetoric to resist international norms "in order to avoid charges of norm violation or to resist pressures for compliance".[123] In this section I briefly summarise how each manoeuvre complements norm-based alternatives.

The first moral manoeuvre, *alignment*, has strong affinities with work on transnational advocacy networks. This is partly because the regional expert community rarely engages with human rights values, and so for this moral manoeuvre I also examine cybersecurity experts in the US and Europe who focus on Egypt and the Gulf states, especially after the Arab Spring. These actors could be – and have been – described as norm entrepreneurs, especially as their actions led to the amendment of the Wassenaar Arrangement, a clear example of a cyber norm. However, there are key differences between alignment and norm entrepreneurship: for example, these experts consciously reject the position of other civil society human rights advocates. More importantly, the moral manoeuvre of alignment emphasises how, because NGOs and their opponents both took the *prima facie* relevance of human rights values for granted, cybersecurity experts altered technical claims to enable human rights values to mirror the existing organisational cluster of values in cybersecurity.

The second moral manoeuvre, *appropriation*, is also not entirely captured by existing norms theories. While norms scholars have argued that states can resist or adapt to international norms pressed upon them by the international community, the role of the Budapest Convention in Egypt and the Gulf states fits neither account. On one hand, none of these states has acceded to this

[121] Alan Bloomfield, 'Norm Antipreneurs and Theorising Resistance to Normative Change', *Review of International Studies* 42, no. 2 (April 2016): 310–33.
[122] Clifford Bob, *The Global Right Wing and the Clash of World Politics* (New York: Cambridge University Press, 2012).
[123] Jennifer M. Dixon, 'Rhetorical Adaptation and Resistance to International Norms', *Perspectives on Politics* 15, no. 1 (March 2017), p.84.

convention, implying resistance, and yet they sometimes claim it to be a key influence on their cybercrime laws *despite* changing those laws to focus on political opposition. Appropriation is a term used by some norm scholars to describe changes made by states to norms more generally.[124] Here I use it to specify the expansion of the professional discourse to fit a particular cluster of values; namely, a broad definition of national security historically prevalent in the region. This moral manoeuvre provides a detailed account both of how states, in Grigsby's words, "cherrypick the norms they want to follow", *and* how they also cherrypick the values and technical claims surrounding those norms.[125]

The third moral manoeuvre, *manipulation*, describes dynamics that are not contained in norm-based accounts of socialisation or compliance. To start with, its focus on surveillance suppliers in the private sector and exporting states who are part of the Wassenaar Arrangement moves beyond most norm theories, as neither actors are recipient states in relation to this norm. Also, by including exporting states as economically motivated actors, this moral manoeuvre also expands the work of Erskine and Carr, who claim only that "the underlying values of the private sector are oriented around the need to maximise profits".[126] Crucially, norm-based accounts of socialisation do not adequately incorporate the extent to which surveillance suppliers are both active participants in shaping as well as responding to cybersecurity norms. The crux of the difference between manipulation and socialisation is whether there is what Finnemore and Hollis call a 'continuum of norm acceptance'. As they describe it:

> Over time, tactical concessions may be made by states resisting the norm; that is, they may minimally conform for instrumental reasons, paying lip service to the norm to satisfy promoters, without actually changing beliefs or engaging in any more norm-conforming behaviour than necessary. This tactical or insincere conformity may continue for some time, but if compliance continues, interactions may move toward dialogue, with persuasion and different forms of socialisation taking centre stage.[127]

[124] Zimmermann, *Global Norms with a Local Face*, pp.217-222.
[125] Grigsby, 'The End of Cyber Norms', p.115.
[126] Erskine and Carr, 'Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace', p.97.
[127] Finnemore and Hollis, 'Constructing Norms for Global Cybersecurity', p.455.

The moral manoeuvre of manipulation breaks the 'continuum of norm acceptance', rather than being a midway point in a larger socialisation process. Although I show that international norms do exert some pressure on international surveillance suppliers, this pressure is limited, avoided and above all productively redeployed in service of their own goals. Consequently, manipulation is more than tactical or insincere conformity, as it proactively creates new institutions around abuse and misuse rather than simply responding passively to norm entrepreneurship. These institutions build in a flexible and agnostic orientation to several value clusters to redefine compliance and maintain sales of surveillance software.

The fourth moral manoeuvre, *elision*, has no clear alternative norm-based explanation, as it focuses on actors not within the scope of the cyber norms above, especially the Wassenaar Arrangement. These actors are specialised cybersecurity companies (whose activities are deliberately excluded); local telecoms companies (who engage in surveillance but do not export it); and local surveillance suppliers and resellers (who are not based in countries covered by the Arrangement). This moral manoeuvre involves the creation of portable concepts that move easily between commercial and national security environments, minimising contradictions between the relevant values in these environments to maximise profits. The nearest norm-based account to elision sees private actors simply as creating new norms, for example in Microsoft's Digital Geneva Convention. Hurel and Lobato challenge a simple view of Microsoft as a 'norm entrepreneur', concluding that "Microsoft's case is not so much indicative of a successful cyber norm enterprise, but of another window that is slowly opening for private actors in the norm debate".[128] The moral manoeuvre of elision suggests that thinking outside the theoretical prism of norm studies opens many more windows for private actors to alter values in cybersecurity.

***

[128] Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs', *Journal of Cyber Policy* 3, no. 1 (27 April 2018), p.11.

In conclusion, this theoretical chapter has argued that this thesis builds on and provides a complement to both critical security studies and norm studies in cybersecurity through three key claims: the central role of an ambiguous expert discourse, the concept of moral manoeuvres itself, and the classification of moral manoeuvres using a distinction between invested and agnostic actors. This thesis thus follows the suggestion made by Risse and Sikkink in the updated version of their pathbreaking book on norms in international politics, where they conclude that "dealing with diverse… issues and different types of target actors will require diverse theoretical and policy approaches".[129] To use a game analogy, moral manoeuvres are a multiplayer computer game. There are shifting teams, alliances, and areas of contest; moves are simultaneous not sequential; definitions of success are liable to change and are not the same for every player; and, of course, there are shortcuts, cheats, and hacks. More vividly, given Bauman's description of modern politics as essentially "liquid", one could view the task at hand as an examination of its fluid dynamics in the case of cybersecurity.[130]

[129] Risse, Ropp, and Sikkink, *The Persistent Power of Human Rights*, p.276.
[130] Zygmunt Bauman, *Liquid Modernity* (Cambridge, UK: Malden, MA: Polity Press, 2000).

Chapter 3: Regions

This chapter argues that cybersecurity can be usefully studied through a regional lens and that Egypt and the Gulf states constitute a region for cybersecurity. I first use IR theories of regions to specify the geographical boundaries of this thesis, excluding other parts of the Middle East that are cybersecurity centres in their own right, and the temporal boundaries, placing the beginning of the empirical analysis at the Arab Spring in 2011 and the end at the Qatar crisis in 2017. This chapter then considers differences between Egypt and the Gulf states in four areas crucial to the argument of this thesis: state formation, communications technologies, human rights, and political developments 2011-2017. Finally, this chapter details the hybrid position of Egypt and the GCC states in international cybersecurity governance, arguing that Egypt and the GCC espouse neither a pure 'cyber sovereignty' nor 'multistakeholder' model. This is due to their longstanding association with the ITU on the one hand and close security links with Western states on the other. This creates a contradictory set of pressures on cybersecurity in the region that facilitates the moral manoeuvres in Part 2.

3.1 Regions and cybersecurity

At first sight, cybersecurity seems unsuited to a regional analysis. The digital communications technologies that comprise the base layers of the internet are global in a mundane sense. Like earlier revolutionary communications technologies, internet communications travel through cables stretching around the world and through space between masts and satellites. Furthermore, their fundamental protocols are not designed to recognise states or regions, understood simply as clusters of geographically proximate states, as these protocols direct packets of data along a constantly changing definition of the most efficient path according to server and cable capacity. The technologies built on these protocols enable almost instantaneous communication between people on opposite sides of the world, enabling a level of coordination, information sharing, and societal integration that is qualitatively different to those afforded by previous communications

technologies, and often called 'globalisation'.[131] Consequently, as all definitions of cybersecurity associate it with the internet and digital communications, this sketch suggests that cybersecurity can only be understood as a global rather than a regional issue.

However, the simple globalisation story overstates the deterritorialisation of international politics for many issue areas, not least cybersecurity.[132] The internet infrastructure is highly influenced by state actions, both within international internet governance bodies and through domestic strategies, laws, surveillance and censorship. It is also shaped by the commercial decisions of multinational companies, who install, maintain, and expand the internet infrastructure for profit within the constraints of the international political economy and often strong national ties. Consequently, even if the types of relationships between states and companies shift in the digital era, national and regional factors remain important.

Regions are geographic entities, although this does not imply that they are natural or fixed. Instead, they are co-constituted by both human and non-human factors.[133] To paraphrase Cox's insight regarding IR theory, regions are always created "for someone and for some purpose".[134] Egypt and the Gulf states are usually placed within the 'Middle East' region, also including (at least) North Africa, the Levant, Turkey, and the east side of the Persian Gulf. However, the Middle East itself is a contested and amorphous region. Although it has a long lineage, the term 'Middle East' gained prominence early in the twentieth century, and in the following decades almost entirely replaced colonial concepts of the Orient and the Near East.[135] This process was intimately connected with imperial and neo-imperial efforts to understand and exert influence over the Islamic world.[136]

---

[131] David Goldblatt et al., *Global Transformations: Politics, Economics, Culture* (Cambridge, UK: Polity Press, 1999).
[132] Paul Hirst, Grahame Thompson, and Simon Bromley, *Globalization in Question* (Cambridge: Polity Press, 2009).
[133] Mary Farrell, Björn Hettne, and Luk Van Langenhove, eds., *Global Politics of Regionalism: Theory and Practice* (London; Ann Arbor: Pluto Press, 2005).
[134] Robert W. Cox, 'Social Forces, States and World Orders: Beyond International Relations Theory', *Millennium* 10, no. 2 (1 June 1981), p.128.
[135] Michael E. Bonine, Abbas Amanat, and Michael Ezekiel Gasper, eds., *Is There a Middle East?: The Evolution of a Geopolitical Concept* (Stanford, California: Stanford University Press, 2011).
[136] Zachary Lockman, *Contending Visions of the Middle East: The History and Politics of Orientalism* (Cambridge, UK; New York: Cambridge University Press, 2009).

In cybersecurity, 'Middle East' is not always understood in the sense used by IR scholars, as many cybersecurity companies adopt both wider and narrower perspectives. On one hand, company structures often include a 'EMEA' branch (Europe, the Middle East and Africa), absorbing the Middle East into a broad negative sales-based definition (i.e. neither the US nor Asia); on the other hand, 'Middle East' conferences, products and events rarely stray beyond Egypt and the GCC, as detailed in the next chapter. Given this plasticity, I distinguish between four different theoretical approaches to the concept 'region' to understand exactly how Egypt and the Gulf states form a region in cybersecurity.

The first approach to regional analysis focuses on supra-state institutions or organisations, rather than simply seeing international dynamics at the level of states or global structures. The Middle East is often considered exceptional for its *lack* of development of regional institutions and their relative ineffectiveness (including in the creation and implementation of norms) when such institutions do exist. Examples include the League of Arab States (LAS) and the Organisation of Islamic Cooperation (OIC), as well as attempts to form regional federations or alliances, such as the Baghdad Pact and the United Arab Republic. Although both the LAS and the OIC have taken limited cybersecurity measures (e.g. creating a facility for sharing information about cybersecurity threats), these organisations do not play a major role in cybersecurity, and so I do not take this approach to regional analysis. Nonetheless, regional branches of international organisations, including the UN's International Telecommunications Union (ITU) 'Arab Region', have shaped the emergence of cybersecurity, and the ITU is considered in the third section of this chapter. There is also a regional 'Arab Convention on Cybercrime', explored in Chapter 7.

The second and third approaches to regional analysis both focus on security, following the standard IR assumption that states fundamentally seek security or at least engage in processes of securitisation. The second approach is 'regional security complex theory', which holds that dynamics of securitisation, including threat construction, can operate at a regional level between certain groups of states. In these cases, Buzan and Waever argue that these states form a 'regional security complex', where their perceptions of security are interdependent even if not all members of a

regional security complex *agree* on security threats.[137] The Middle East as a regional security complex has been analysed extensively, with several 'subcomplexes' (for example, in the Persian Gulf).[138] It is possible to apply this approach in cybersecurity by identifying a 'regional cybersecurity complex'. An initial sketch of such a complex would see Egypt and the Gulf states as one side of a triangle of cybersecurity actors in the Middle East, each of whom has conducted significant cyber operations both within and outside its borders, and possesses a range of cybersecurity structures and capabilities. The other two sides of this triangle are Iran and Israel (Turkey does not meet these criteria), and I consider them briefly here.

Iran is seen by many as a geopolitical rival to Saudi Arabia, partly due to its support to armed groups in Yemen and Syria, although a broader antagonism is popularly conceived as starting after the 1979 Iranian revolution. However, Iran has more ambiguous relationships with other Gulf states: Bahrain, with a large Shia population, has close historic links to Iran; Oman has a longstanding policy of neutrality and brokered the 2015 Iranian nuclear agreement; while northern UAE emirates (excluding the capital, Abu Dhabi) and Qatar have extensive economic ties with Iran. Most notable cybersecurity incidents in the Middle East have occurred in relation to the Iranian nuclear programme, from a famous US-Israeli operation aiming to disrupt Iranian uranium enrichment (named 'Stuxnet'),[139] to Iranian cyber operations against US banks in response to sanctions in 2012, and Israeli cyber espionage on the nuclear negotiations themselves. Iran has a mature cybersecurity capability, with loose and transient relationships between commercial companies and military organisations.

Israel, in contrast to Iran, is a global cybersecurity hub in its own right, with a strong military-based cybersecurity sector and high-value exports worldwide.[140] Israel has been in conflict with and politically isolated from the Arab world since its creation, although covert cooperation now exists in

[137] Barry Buzan and Ole Waever, *Regions and Powers: The Structure of International Security* (Cambridge; New York: Cambridge University Press, 2003).
[138] Matteo Legrenzi and Cilja Harders, eds., *Beyond Regionalism?: Regional Cooperation, Regionalism and Regionalization in the Middle East* (Oxford: Routledge, 2008).
[139] Kim Zetter, *Countdown to Zero Day* (New York: Penguin Random House, 2014); David E. Sanger, *Confront and Conceal* (New York: Penguin Random House, 2013).
[140] Richard Behar, 'Inside Israel's Secret Startup Machine', Forbes, 11 May 2016, https://perma.cc/L7EH-8ZZ4.

various cybersecurity-related areas.[141] In particular, Egypt and Israel have shared digital intelligence in the Sinai Peninsula, where there is a Islamic State-affiliated terrorist threat, and the Gulf states have sourced many security technologies from Israel. Overall, Iran and Israel can be seen as two sides of a regional cybersecurity complex including Egypt and the Gulf states, with mutually interdependent securitisation processes. Their actions in cybersecurity will appear periodically throughout the empirical chapters as both threats and security partners, but they are not the main focus of this thesis.

The third variant of regional analysis is also based on the security-seeking character of states, but posits that states with similar security interests form 'security communities', where they resolve disputes using peaceful means, and face joint threats in a more integrated manner than formal alliances.[142] The nearest institution to a security community in the Middle East is the GCC itself, formed in 1981 shortly after the Iranian revolution. However, in Barnett and Gause's evaluation, the GCC is "little more than a classic military alliance", despite a period of increased cooperation after the 1990-91 Gulf War, when a GCC state (Kuwait) was invaded by Iraq.[143] More recent studies of the GCC have indicated that the GCC remains divided and unlikely to form serious security cooperation in future (especially after the Qatar crisis, considered below).[144] The few existing analyses of cybersecurity in the GCC highlight these structural problems.[145]

Egypt's relations with the GCC also do not constitute a security community. Although Egypt has historically conducted several military interventions on the Arabian Peninsula, and had conflictual relations with the Gulf states during the early Cold War, since the GCC's creation

[141] Ben Caspit, 'The Israeli-Egyptian Love Affair', Al-Monitor, 29 February 2016, https://perma.cc/N8EH-8G42; Rori Donaghy, 'Falcon Eye: The Israeli-Installed Mass Civil Surveillance System of Abu Dhabi', Middle East Eye, 28 February 2015, https://perma.cc/3WX8-XMM5.
[142] Emmanuel Adler and Michael N. Barnett, eds., *Security Communities* (Cambridge; New York: Cambridge University Press, 2008).
[143] Michael Barnett and F. Gregory III Gause, "Caravans in Opposite Directions: Society, State and the Development of a Community in the GCC," in *Security Communities*, ed. Emmanuel Adler and Michael Barnett (Cambridge, UK; New York: Cambridge University Press, 2008), 161–97.
[144] Matteo Legrenzi, *The GCC and the International Relations of the Gulf: Diplomacy, Security and Economic Coordination in a Changing Middle East* (I.B.Tauris, 2015), pp.74-76; Khalid Almezaini and Jean-Marc Rickli, eds., *The Small Gulf States* (London; New York: Routledge, 2016).
[145] Nir Kshetri, 'Cybersecurity in the Gulf Cooperation Council Economies', in *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (New York, NY: Springer, 2016), 183–94; James Andrew Lewis, 'Cybersecurity and Stability in the Gulf' (Center for Strategic & International Studies, January 2014), https://perma.cc/ST48-NVGX.

relations with Egypt have been primarily economic (a GCC+2 including Egypt and Syria was mooted with no tangible result after the Gulf War). Crucially, there is no indication that a regional cybersecurity community – understood as friendly relations between security-seeking states – has emerged in the Middle East, including in Egypt and the GCC. How, then, can these be treated as a cybersecurity region?

The fourth and final variant of regional analysis includes 'regionalisation', a term that describes the intensification of regional processes, including security, economic and cultural associations. Fawcett and Hurrell distinguish regionalism (the region as a normative goal) from regionalisation (the occurrence of regional processes).[146] Fawcett suggests that we need an "expansive and flexible" concept of the region to avoid the strict classifications of state-based security complexes and communities in IR,[147] and a multilevel understanding of the Middle East in particular.[148] This, for me, is the most fruitful approach to regional analysis, and I treat Egypt and the Gulf states as a cybersecurity region for two reasons, both explored in more detail later in the thesis. First, there is a transnational cybersecurity *expert* community across Egypt and the Gulf states, rather than a regional security community of like-minded states (the subject of Chapter 4). Second, Egypt and the Gulf states occupy a hybrid position in the bipolar international internet governance architecture (the subject of the last section of this chapter). The key point is that both are regional features connecting Egypt and the Gulf states *in cybersecurity*. This does not imply that Egypt and the Gulf states deserve a regional analysis in all issue areas.

A regional approach to cybersecurity does not require the complete exclusion of factors outside the region. Instead, I include actors and processes elsewhere insofar as they affect cybersecurity in Egypt and the Gulf states. Given the globalising trends mentioned above, including the ability to trade, monitor and lobby from anywhere in the world, several external elements are crucial to my analysis. In Part 2 I examine the role of NGOs based in Canada and the US, surveillance

[146] Louise Fawcett and Andrew Hurrell, eds., *Regionalism in World Politics: Regional Organizational and International Order* (New York: Clarendon Press, 1996), p.39.
[147] Louise Fawcett, 'Exploring Regional Domains: A Comparative History of Regionalism', *International Affairs* 80, no. 3 (1 May 2004), p.431.
[148] Louise Fawcett, 'Alliances and Regionalism in the Middle East', in *International Relations of the Middle East*, ed. Louise Fawcett (Oxford: Oxford University Press, 2013), 197–217.

suppliers and export regulations in the US and Europe, and multinational companies operating worldwide. The caveat imposed by a regional analysis is that such actors may well engage in similar activities elsewhere in the world similar to those examined here, which are beyond the scope of the thesis.

A regional analysis also provides the justification for the time period selected for this thesis: 2011-2017. The so-called 'Arab Spring' in 2011, a series of protests beginning in Tunisia and spreading across the Middle East, marks a key juncture in the long-term political fabric of the Middle East. Although the Arab Spring was embraced by many observers as heralding a delayed turn to democracy in the Arab world, this proved to be overstated: in 2018, only Tunisia retained a credibly elected government after the protests. Nonetheless, 2011 is an appropriate starting point for a study of cybersecurity in the region, especially in Egypt and the Gulf states, as questions of internet communications, social media, and critical infrastructure took on new meanings for both governments and opposition movements after 2011. I provide an overview of the specific political developments in Egypt and the GCC states in the next section.

The end of the time period considered by the study is the June 2017 Gulf crisis. On 05 June 2017, Bahrain, Egypt, Saudi Arabia and the United Arab Emirates (the 'quartet') ostracised Qatar by recalling citizens, withdrawing ambassadors, ceasing all land, air, and sea links and beginning an economic boycott. Although a few other countries joined the quartet, the main international allies of the GCC remained neutral. This split has increased ties between Qatar and Oman and set back the Gulf Cooperation Council (GCC) considerably. It also drew Egypt closer to the other quartet states and caused the withdrawal of Qatar from its minor role in Yemen due to Saudi Arabia's leadership of the coalition forces. This split follows a long cycle of dispute and reconciliation between Qatar and its neighbours. The origin of this split (a likely hack of Qatar News by the UAE or Saudi Arabia) is examined in the thesis conclusion. June 2017 can be seen as a convenient punctuation mark in the politics of Egypt and the Gulf states, rather than a clear cessation of the patterns examined in this thesis.

Finally, one other anomaly must be noted. Yemen is not included in the analysis, despite being an Arab state on the Arabian Peninsula, albeit not in the GCC. Yemen has been the site of a devastating civil war since 2015, in which all the GCC states are intimately involved (Oman, although not part of the Saudi-led coalition, has run intelligence and border security operations in Yemen). These relationships are not always cooperative: Qatar has withdrawn since the crisis in 2017, while the UAE and Saudi Arabia have supported different armed groups. Yemen has very different cybersecurity issues, as it is the site of extensive intelligence operations for the coalition and their partners in the UK and US, as well as US special forces operations and the actions of Iranian-supported militias.[149] The suffering due to war, famine and disease in Yemen raises entirely different questions to those considered here.

In sum, this section has established that a regional approach to cybersecurity is possible and suggested that Egypt and the Gulf states form a region in cybersecurity according to an understanding of regionalism that focuses on regional-level processes and features, rather than the creation of a regional security complex or state-based security community. These cybersecurity-specific regional factors, explored later in this chapter and in Chapter 4, justify the regional approach to moral manoeuvres in Part 2.

3.2 Intra-regional differences

Although we can consider Egypt and the Gulf states as a region *for cybersecurity*, this does not imply that such a configuration would be apt for all issue areas, or that these states are homogeneous in their political and social developments. Of course, Egypt and the six GCC states each have varied histories, economies, and societies. The scope of this thesis does not permit more than a brief consideration of the wider history and context of the region, and it cannot do justice to the complexities of the individual states and peoples. In this section, I consider four differences: first, state formation; second, communications technologies; third, human rights; and fourth, political

[149] Jakub Dalek et al., 'Information Controls During Military Operations The Case of Yemen' (Citizen Lab, 21 October 2015).

developments 2011-2017. These differences are essential to the thesis argument, as the cluster of values around an expansive definition of national security which features in Part 2 can be understood only in light of the individual socio-technological context and historical position of each state.

3.2.1 State formation

The political systems of Egypt and the Gulf states have been partly determined by their varied paths into the modern international system over the last two centuries. Egypt experienced both British and French colonial influence, as commercial competition between the two colonial powers preceded British occupation in 1882.[150] The extensive control of British officials over state decisions (the 'veiled protectorate') was followed by the formal declaration of a protectorate in 1914 and continued exercise of British influence in a turbulent political scene following the 1919 revolution.[151] Although Egypt officially became independent in the Anglo-Egyptian Treaty of 1936, it was re-occupied by Allied forces during World War II. After the deposition of King Farouk in 1952 by a group of military officers including then-Lieutenant-Colonel and later President Gamal ʿAbdel Nasser, the latter pursued a policy of pan-Arabism with divisive effects for the wider region.[152] Egypt held a key strategic position in the Cold War, as a prized ally first of the Soviet Union and then the US, as well as playing a decisive role in the Arab-Israeli conflict.[153] Throughout this period, the Muslim Brotherhood (formed by Hassan Al-Banna in 1929) created a fissure in Egyptian politics over political Islam, with periodic repression under Nasser and relative freedom under his successor in 1970, President Anwar Sadat.[154]

---

[150] Timothy Mitchell, *Colonising Egypt* (Berkeley: University of California Press, 1992); Eugene Rogan, *The Arabs: A History* (Penguin, 2012), pp.129-140.
[151] P. J. Vatikiotis, *The History of Modern Egypt: From Muhammad Ali to Mubarak* (London: Weidenfeld & Nicolson, 1991), pp.249-272; James Whidden, *Monarchy and Modernity in Egypt: Politics, Islam and Neo-Colonialism Between the Wars* (London; New York: I.B.Tauris, 2013).
[152] Michael N. Barnett, *Dialogues in Arab Politics: Negotiations in Regional Order* (New York: Columbia University Press, 1998); Michael Doran, 'Egypt: Pan-Arabism in Historical Context', in *Diplomacy in the Middle East: The International Relations of Regional and Outside Powers*, ed. L. Carl Brown (London; New York: I.B.Tauris, 2003), 97–120.
[153] Hugh Wilford, *America's Great Game* (New York: Basic Books, 2014), pp.133-159.
[154] Nazih Ayubi, *Political Islam: Religion and Politics in the Arab World* (London: Routledge, 1993), pp.54-65.

Sadat's 'infitah' in the 1970s opened the Egyptian economy to foreign investment, aiming to ameliorate Egypt's longstanding structural economic problems and extensive poverty in its large population (around 90 million in 2018). Following the assassination of Sadat in 1981, the new President Hosni Mubarak won multiple elections with significant levels of popular support, but these elections were also criticised for their procedural irregularity and coercive tactics by Mubarak's National Democratic Party. Egypt remained a target for international development, and Mubarak's cooperation with the US in security and defence was rewarded with several substantial US aid programmes.[155] This aid and foreign investment was distributed among senior state officials and favoured business partners in what has been referred to as 'crony capitalism'.[156] Overall, the Egyptian political system has been characterised by military-affiliated authoritarian leaders within an energetic parliamentary system with limited independence.[157]

The path of the Gulf states into the modern international system was very different to that of Egypt. British colonial policy in the Gulf was to 'uphold the independence' of the ruling families, but ensure that British influence 'remained supreme',[158] and treaties to guarantee the safety of British shipping to India were signed with the littoral states (hence the 'Trucial' states) throughout the nineteenth century.[159] This sea trade built on longer histories of port cities in the Gulf as cosmopolitan entrepôts.[160] Saudi Arabia has a distinct history within the Gulf.[161] Throughout the first half of the twentieth century, ʿAbdulaziz Al-Saud (known as Ibn Saud) expanded his territory in central Arabian peninsula (the Najd) with the cooperation of clerics following the Islamic teachings of Muhammad Al-Wahhab, as well as the co-option of an armed tribal force of the Ikhwan ('brotherhood'), and

[155] Timothy Mitchell, *Rule of Experts: Egypt, Techno-Politics, Modernity* (Berkeley: University of California Press, 2002), p.240.
[156] Clement Moore Henry and Robert Springborg, *Globalization and the Politics of Development in the Middle East* (New York: Cambridge University Press, 2010), p.154.
[157] Robert Springborg, *Egypt* (Cambridge, UK: Polity Press, 2017); Steven A. Cook, *The Struggle for Egypt: From Nasser to Tahrir Square* (Oxford: Oxford University Press, 2013); Hazem Kandil, *The Power Triangle: Military, Security, and Politics in Regime Change* (Oxford: Oxford University Press, 2016).
[158] Lord Curzon cited in Sean Foley, *The Arab Gulf States: Beyond Oil and Islam* (Boulder, Colo: Lynne Rienner Publishers, 2010), p.16.
[159] Rosemary Said Zahlan, *The Making of the Modern Gulf States: Kuwait, Bahrain, Qatar, the United Arab Emirates and Oman* (Ithaca: Ithaca Press, 1998), p.20.
[160] Laurence Potter, ed., *The Persian Gulf in Modern Times: People, Ports, and History* (New York: Palgrave Macmillan, 2014).
[161] Tim Niblock, *Saudi Arabia: Power, Legitimacy and Survival* (London: Routledge, 2006); Tim Niblock and Monica Malik, *The Political Economy of Saudi Arabia* (Oxford; New York: Routledge, 2007).

British consent.[162] Ibn Saud formally established the state of Saudi Arabia in 1932, although, for Saudi historians, this is officially the third Saudi state, as earlier attempts to unify the Arabian peninsula under Saudi ancestors in the eighteenth and nineteenth centuries failed due to internal opposition and Ottoman military intervention.[163] The retreat of British imperial power after World War II precipitated a late wave of state formation: the Al-Sabah of Kuwait declared independence in 1961, while the ruling families north of Oman formed the states of the United Arab Emirates (chiefly Al-Nahyan in Abu Dhabi and Al-Maktoum in Dubai), Qatar (Al-Thani) and Bahrain (Al-Khalifa) in 1971 following official British withdrawal. Sultan Qaboos of Oman came to power after a British-organised coup against his father in 1970, and the suppression of a rebellion in Dhofar, the southern province bordering Yemen, between 1970 and 1977.[164]

These states are all much smaller than Egypt, some drastically so, with populations of around 30 million in Saudi Arabia and less than 3 million in Qatar. Their population and infrastructure grew rapidly after the discovery of oil and gas reserves across the Persian Gulf and Arabian Peninsula, with multinational companies and high levels of migrant labour affecting both economy and society.[165] The GCC economic model has been described as 'rentier state', in which citizens (a narrow definition tied to the male line of descent) receive many benefits from extractives revenue.[166] However, this model has been challenged by analyses that demonstrate the continuing economic importance of the private sector and state bureaucracies.[167] Overall, the GCC states have neo-patrimonial systems of monarchical government, in which male members of the ruling family control key government departments and maintain influence in many private sector organisations. The

[162] Madawi Al-Rasheed, *A History of Saudi Arabia* (New York: Cambridge University Press, 2010).
[163] Jorg Matthias Determann, *Historiography in Saudi Arabia: Globalization and the State in the Middle East* (London; New York: I.B.Tauris, 2013), pp.24-38.
[164] Francis Owtram, *A Modern History of Oman: Formation of the State since 1920* (London; New York: I.B.Tauris, 2004); Mark Valeri, *Oman: Politics and Society in the Qaboos State* (C Hurst & Co Publishers Ltd, 2017).
[165] Robert Vitalis, *America's Kingdom: Mythmaking on the Saudi Oil Frontier* (London: Verso Books, 2009); Daniel Yergin, *The Prize: The Epic Quest for Oil, Money & Power* (London; New York: Simon & Schuster, 2009); Timothy Mitchell, *Carbon Democracy: Political Power in the Age of Oil* (London: Verso Books, 2013).
[166] Hazem Beblawi and Giacomo Luciani, eds., *The Rentier State* (Routledge, 2016).
[167] Steffen Hertog, 'Defying the Resource Curse: Explaining Successful State-Owned Enterprises in Rentier States', *World Politics* 62, no. 2 (April 2010): 261–301; Steffen Hertog, 'The Private Sector and Reform in the Gulf Cooperation Council' (Kuwait Programme on Development, Governance and Globalisation in the Gulf States, July 2013); Steffen Hertog, *Princes, Brokers, and Bureaucrats: Oil and the State in Saudi Arabia* (Ithaca: Cornell University Press, 2011).

degree of consultation in government differs across the GCC: Kuwait has a relatively independent parliament, and Bahrain has had several interrupted periods of parliamentary government.[168] There are less powerful bodies elsewhere in the Gulf, including consultative councils or assemblies in Oman, UAE, Qatar, and Saudi Arabia. Leadership is based partly on co-option of potential threats, and partly on narratives that associate leaders with state creation, tribal authority, and Islam.[169] Internationally, GCC capital is very influential, and their sovereign wealth funds and expatriates play an important part in many world economies. For some, the UAE especially, liberalised city-states have provided a haven for global capital.[170] All the oil states have used their productive capacity strategically as members of the Organisation for Petroleum Exporting Countries, most visibly around the Arab-Israeli war in October 1973 (often simplistically described as an 'oil weapon').[171] Oil wealth has also been the basis of massive arms sales to guarantee Gulf security, especially after the 1990-91 Gulf war.

In sum, these differing paths of state formation have led to both an expansive definition of national security shared across these states and variations in this definition for particular industries, organisations and elite groups.

3.2.2 Communications technologies

Modern communications technologies have drastically transformed this region. Egypt's strategic use of communications technologies is commonly illustrated by the use of regional radio to promote Nasser's policy of pan-Arabism in the 1950s and 1960s. Much later, the establishment of

[168] Fred Haley Lawson, *Bahrain: The Modernization of Autocracy* (Westview Press, 1989); Shaul Yanai, *Political Transformation of Gulf Tribal States: Elitism & the Social Contract in Kuwait, Bahrain & Dubai, 1918-1970s* (Brighton: Sussex Academic Press, 2014); Miriam Joyce, *Bahrain from the Twentieth Century to the Arab Spring* (New York: Palgrave Macmillan, 2012).
[169] Andrea B. Rugh, *The Political Culture of Leadership in the United Arab Emirates* (Basingstoke: Palgrave Macmillan, 2010); Christopher M. Davidson, *The United Arab Emirates: A Study in Survival* (Lynne Rienner Publishers, 2005).
[170] David Held and Kristian Ulrichsen, eds., *The Transformation of the Gulf: Politics, Economics and the Global Order* (Oxford; New York: Routledge, 2011); Christopher M. Davidson, *Dubai: The Vulnerability of Success* (London: Hurst, 2009).
[171] Mitchell, *Carbon Democracy*, p.175.

Egypt's first internet connection in 1993 was due to a few charismatic individuals and a small, well-educated agency outside central government.[172] Internet penetration was very low outside Cairo and Alexandria, and internet access became a core development item.[173] As with previous technologies, this was both a blessing and a curse: the attention of international businesses, consultancies and agencies often benefited themselves as much as or more than their targets, creating what has been termed 'asymmetrical development' of the internet.[174] The development of the internet in Egypt has had significant effects not just on its ability to attract global economic interest, but also on the self-image of Egyptians themselves in forming new social movements, both explicitly political and in other arenas.[175]

The Gulf states installed their first internet connections in the mid-1990s, with national agencies in charge.[176] Initially, these connections were provided by satellite, and endpoints were in university departments and hospitals who wanted connectivity with their international research partners. Major undersea cables in 1998 and 1999 provided wider connectivity and were funded by national and multinational telecoms companies. The introduction of these technologies changed the way people in these states interacted, especially over gender and social divides. This included the internet cafe, where domestic pressures were relieved, and later the internet-enabled mobile phone (although camera-enabled mobiles again attracted an attempted ban by the Saudi government in 2002).[177] Internet penetration rates for the Gulf were consistently the highest in the region, and the Gulf states all took steps towards e-government in the new millennium.

---

[172] Nivien Saleh, *Third World Citizens and the Information Technology Revolution* (London; New York: Palgrave MacMillan, 2010).
[173] Deborah L. Wheeler, 'Egypt: Building an Information Society for International Development', *Review of African Political Economy* 30, no. 98 (1 December 2003): 627–42.
[174] Ilhem Allagui, 'Internet in the Middle East: An Asymmetrical Model of Development', *Internet Histories* 1, no. 1–2 (2 January 2017): 97–105.
[175] Rasha A. Abdulla, *The Internet in the Arab World: Egypt and Beyond* (New York: Peter Lang Publishing, 2007).
[176] Jon W. Anderson, 'Producers and Middle East Internet Technology: Getting beyond "Impacts"', *Middle East Journal* 54, no. 3 (2000): 419–31.
[177] Deborah L. Wheeler, *The Internet In The Middle East: Global Expectations And Local Imaginations In Kuwait* (Albany: State University of New York Press, 2005).

The treatment of new communications technologies must be considered in the context of information control and censorship.[178] Censorship was extensive in most Arab countries in the latter half of the twentieth century. It was both official and informal, external and self-imposed, and applying to both media and wider public spheres.[179] State ownership of the media enabled direct and immediate control, supported by broad laws capturing many kinds of critical speech.[180] While Kuwait had an early open press, the other Gulf states remained 'loyalist', to use Rugh's term.[181] Responses varied widely to the introduction of new communications technologies in the 1990s. While Saudi Arabia banned satellite dishes and selectively confiscated signal decoders from citizens for companies that broadcast critical programmes, the UAE adopted an 'open-skies' approach and proclaimed a policy promoting freedom of expression (although its practice did not match these claims).[182] The watershed moment for censorship was the 1991 Gulf War, which was entirely absent from most national broadcasters in the Gulf states. The only coverage was provided by the US channel Cable News Network (CNN) and widely watched. Qatar then modelled on CNN the pathbreaking current affairs channel Al-Jazeera, leading to a range of professionally packaged media initiatives across the Gulf, especially in Saudi Arabia.[183] The Gulf states also exercised significant influence on media production in neighbouring states, due to the revenues media companies in those states collected from viewers in the Gulf. Finally, Saudi Arabia and other Gulf states used the difference between placid local media and aggressive state-supported foreign channels to project regional standing and maintain domestic narratives of authority.[184]

---

[178] Emma C. Murphy, 'Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere', *International Studies Quarterly* 53, no. 4 (1 December 2009): 1131–53.
[179] Emma C. Murphy, 'Agency and Space: The Political Impact of Information Technologies in the Gulf Arab States', *Third World Quarterly* 27, no. 6 (2006): 1059–83; Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, D.C: Brookings Institution Press, 2002).
[180] Edward Webb, 'Holding Back The Flood: Regimes of Censorship in the Middle East & North Africa in Comparative Perspective', *German Media Journal*, no. 2012/01 (May 2012); Eugene Rogan, 'Rise and Fall', *Index on Censorship* 25, no. 2 (1 March 1996): 43–49.
[181] William A. Rugh, *The Arab Press: News Media and Political Process in the Arab World* (Syracuse, N.Y: Syracuse University Press, 1987), p.174.
[182] Naomi Sakr, *Satellite Realms: Transnational Television, Globalization and the Middle East* (London: I.B.Tauris, 2002).
[183] Marc Lynch, *Voices of the New Arab Public: Iraq, Al-Jazeera, and Middle East Politics Today* (New York, NY: Columbia University Press, 2007).
[184] Mohamed Zayani, 'Transnational Media, Regional Politics and State Security: Saudi Arabia between Tradition and Modernity', *British Journal of Middle Eastern Studies* 39, no. 3 (1 December 2012): 307–27.

This censorship is both a product of and a factor in sustaining the expansive definition of national security above. Generally, state control of the media has continued through internet filtering and censorship,[185] despite the potential of internet access to increase political participation and public spheres.[186] Government organisations in all these states have been labelled as 'enemies of the internet' by Reporters without Borders.[187] Early censorship was often obvious, with an option to report unsuitable content; a measure that was designed to placate conservative sections of the population. However, people responded to filtering by finding ways around it, through foreign providers, proxies, and frequent changes to web addresses.

The Gulf states in particular were nonetheless open to the internet as an economic driver, being, in Howard's phrase, "wired for business, but not politics".[188] For example, in Saudi Arabia the internet was not publicly available for five years after the first institutional connections and was only permitted after the government-run King ʿAbdulaziz City for Science and Technology (KACST) assumed responsibility for policing content. KACST and similar agencies in the other Gulf states purchased a range of US-produced internet filtering software, designed for corporations to monitor their employees or families to monitor children, and adapted it to the task of national filtering.[189] Saudi Arabia held an open competition for renewing this contract in 2001, and the US companies competing for this contract – Secure Computing, later owned by McAfee and Intel, and Websense, later owned by Raytheon – were still supplying the region when the media focus returned in 2011. These diverse histories of filtering and censorship play a key role in the moral manoeuvres of alignment and manipulation in Part 2.

---

[185] Kalathil and Boas, *Open Networks, Closed Regimes*; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2012); Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008).

[186] Mamoun Fandy, 'Information Technology, Trust, and Social Change in the Arab World', *Middle East Journal* 54, no. 3 (2000): 378–94; Grey Burkhart and Susan Older, 'The Information Revolution in the Middle East and North Africa' (RAND Corporation, 2003); Jon W. Anderson, 'Is Informationalization Good for the Middle East?', *Arab Media & Society* Summer, no. 18 (12 June 2013); Allagui, 'Internet in the Middle East'.

[187] Reporters without Borders, 'Enemies of the Internet', accessed 1 June 2017, http://12mars.rsf.org/2014-en/.

[188] Philip N. Howard, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam* (Oxford; New York: Oxford University Press, 2010), p.80.

[189] Ahmed Mardini, 'Gulf Internet: Gulf States Move to Police Cyberspace', IPS, 4 April 1997, https://perma.cc/WGC8-3XVY; Jennifer Lee, 'Companies Compete to Provide Internet Veil for the Saudis', *The New York Times*, 19 November 2001, https://perma.cc/QPQ6-PQED.

3.2.3 Human rights

Egypt and the Gulf states have consistently participated in regional and international human rights bodies, Saudi Arabia's abstention from the original 1948 Declaration of Human Rights notwithstanding. Civil and political rights were given international legal force following the International Covenant on Civil and Political Rights (1976), which was ratified by Egypt, Kuwait and Bahrain in 1982, 1996 and 2006 respectively, but not signed or ratified by Saudi Arabia, Oman, Qatar, or the UAE. Nonetheless, these rights are part of customary international law, to which these states are bound. The right prohibiting torture and mistreatment was specifically enshrined by the Convention Against Torture (1987), ratified by Egypt and all Gulf states other than Oman.[190]

In the region, there was a notable attempt to "adopt a pose of human rights with no real sympathy", as Mayer describes the Universal Islamic Declaration of Human Rights in 1981.[191] Later symbolic declarations of commitment to human rights include those by the OIC (1990), the LAS (2004),[192] and most recently the Gulf Cooperation Council (2014). The UN Human Rights Council, formed in 2006, has included Egypt and all the Gulf states other than Oman on three-year rotating chairs. The Council was formed after an earlier version, also including Egypt, Saudi Arabia, and Qatar, was criticised for the inclusion of states with poor human rights records.[193] However, such criticisms continue: Saudi Arabia's seat was secured in part due to alleged vote-trading with the UK,[194] and it has also reportedly used its funding of the council to prevent UN criticism of its military action in Yemen on human rights grounds.[195] Domestically, these governments have also funded national human rights organisations that do not publicise violations identified by independent

[190] Despite significant time differences: Egypt (1987), Kuwait (1996), Saudi Arabia (1997), Qatar (2000), and UAE (2012).
[191] Ann Mayer, *Islam and Human Rights: Tradition and Politics* (Boulder, Colo: Westview Press, 2012), p.37.
[192] This became the Arab Charter on Human Rights; Mervat Rishmawi, 'The Arab Charter on Human Rights and the League of Arab States: An Update', *Human Rights Law Review* 10, no. 1 (1 March 2010): 169–78.
[193] BBC, 'UN Creates New Human Rights Body', 15 March 2006, https://perma.cc/SUQ6-LKAQ.
[194] Owen Bowcott, 'UK and Saudi Arabia "in Secret Deal" over Human Rights Council Place', *The Guardian*, 29 September 2015, https://perma.cc/9CAT-J66L.
[195] Somini Sengupta, 'United Nations Chief Exposes Limits to His Authority by Citing Saudi Threat', *The New York Times*, 9 June 2016, https://perma.cc/3XJ8-GNSK.

bodies.[196] A good example of the conflict over human rights in the region is the Bahraini Commission of Independent Inquiry, formed to investigate human rights violations committed by the Bahraini government in 2011.[197] As it developed, multiple contradictions emerged between claims by NGOs and the chair of the inquiry that its recommendations had not been implemented on the one hand, and claims by the Bahraini, UK and US governments that these recommendations had either been implemented fully or demonstrated sufficient reform on the other.[198]

Communications technologies have been a battleground and tool in the intense conflict over human rights. Journalists have been pressured, imprisoned and killed,[199] while 'Western' technology companies have struggled between their identity as providers of 'technologies of liberation' and their governments' security alliances with these states.[200]

Overall, these governments are judged as having low levels of adherence to certain key human rights, thereby creating a substantial moral distance between them and their predominantly Western human rights observers.[201] Scholars have explored a number of reasons for the extent of human rights violations in this region, including the incompatibility of Islam with the liberal ideas usually associated with human rights.[202] Others have critiqued 'cultural relativist' approaches which explain a supposed lack of engagement with human rights based on essentialist notions of religious

[196] Such bodies include the National Human Rights Council (Qatar, 2002), the National Society for Human Rights (Saudi Arabia, 2004), and the International Gulf Organization for Human Rights (UAE, 2012).
[197] Mahmoud Cherif Bassiouni, 'Report of the Bahrain Independent Commission of Inquiry' (Bahrain Independent Commission of Inquiry, 10 December 2011).
[198] ADHR, 'Dispatch: Fact vs. Myth - Bahrain Independent Commission of Inquiry (BICI)', *Americans for Democracy & Human Rights in Bahrain* (blog), 1 August 2016, https://perma.cc/JH98-MTUN; Ian Black, 'Bahrain Torture Report Undermines UK's Reform Claims', *The Guardian*, 23 November 2015, https://perma.cc/79NA-5RAX.
[199] Rasha A. Abdulla, 'Egypt's Media in the Midst of Revolution' (Carnegie Endowment for International Peace, July 2014).
[200] Gholam Khiabany, 'Technologies of Liberation and/or Otherwise', *International Journal of Middle East Studies* 47, no. 2 (May 2015): 348–53.
[201] For an early activist position, see James Paul and Joe Stork, 'The Middle East and Human Rights', *Middle East Research and Information Project* Winter, no. 149 (1987), https://perma.cc/6D7S-ELJ8; Mayer, *Islam and Human Rights*.
[202] Katerina Dalacoura, *Islam, Liberalism and Human Rights*, (London; New York: I.B.Tauris, 2003); Abd Allah Ahmad Naim, 'The Interdependence of Religion, Secularism, and Human Rights: Prospects for Islamic Societies', *Common Knowledge* 11, no. 1 (11 January 2005): 56–80; Mahmood Monshipouri, *Muslims in Global Politics: Identities, Interests, and Human Rights* (Philadelphia: University of Pennsylvania Press, 2012).

or cultural tradition.[203] Despite this, genuine human rights movements have also developed in these countries over the last century in Egypt, and more recently in the Gulf states.[204] Although these states do not have equivalent approaches to human rights – far from it – I make only the weaker claim that they are all the site of significant human rights violations. The association of these violations with surveillance technologies as a cybersecurity issue is the moral manoeuvre of alignment, detailed in Chapter 6.

3.2.4 Political developments 2011-2017

All four moral manoeuvres in part 2 were performed in the context of significant political change from 2011 to 2017. The Egyptian revolution of January 2011, at the start of this period, is often described as a 'Facebook revolution', highlighting the perceived effects of social media on state power.[205] The Egyptian government shut down internet access altogether in January 2011 following mass protests.[206] Although this process is not as simple as it has been described – as a 'kill switch', considered in Chapter 9 – it was remarkably effective in the short term and lasted for five days, before a combination of popular anger and elite disassociation forced the resignation of President Mubarak.[207] Following Mubarak's resignation, the Supreme Council of the Armed Forced (SCAF) took power for just over a year until the election of Muslim Brotherhood-affiliated

[203] R. J. Vincent, *Human Rights and International Relations* (Cambridge; New York: Cambridge University Press, 1987), pp.42-44; Fred Halliday, *Islam and the Myth of Confrontation: Religion and Politics in the Middle East* (London; New York: I.B.Tauris, 2003), pp.133-159.
[204] Mishana Hosseinioun, 'The Globalisation of Universal Human Rights and the Middle East' (DPhil Thesis, University of Oxford, 2013); Susan E. Waltz, *Human Rights and Reform: Changing the Face of North African Politics* (Berkeley: University of California Press, 1995); Anthony Chase and Amr Hamzawy, eds., *Human Rights in the Arab World: Independent Voices* (Philadelphia: University of Pennsylvania Press, 2008). Notably: the Arab Organization for Human Rights (1983) and its local affiliates, the Committee for the Defense of Legitimate Rights (1993) in Saudi Arabia, and the Arab Network for Human Rights Information (2004).
[205] John Chalcraft, 'Egypt's 25 January Uprising, Hegemonic Contestation, and the Explosion of the Poor', in *The New Middle East: Protest And Revolution In The Arab World*, ed. Fawaz A. Gerges (New York: Cambridge University Press, 2013), p.157.
[206] James Glanz and John Markoff, 'Egypt's Autocrats Exploited Internet's Weaknesses', *The New York Times*, 15 February 2011, https://perma.cc/4WVN-7G8E.
[207] Marc Lynch, *The Arab Uprising: The Unfinished Revolutions of the New Middle East* (New York: PublicAffairs, 2013).

Muhammad Morsi, who ruled in an equally partisan manner, inverting the previous regime's anti-Brotherhood stance.

Continued protests and mass dissatisfaction with Morsi's rule emboldened the armed forces to step in again in July 2013. Defence minister ʿAbdel Fattah Al-Sisi suspended the constitution and removed Morsi from power, initiating violent repression of Morsi supporters and the Muslim Brotherhood more widely, including a massacre of at least 700 individuals at Rabiʿa Al-ʿadawiyya Square in Cairo in August 2013. Following an interim government, Al-Sisi was elected President in May 2014 in disputed and boycotted elections.[208] After the events of 2013 an Islamist insurgency in the Sinai Peninsula swelled, with thousands of casualties and an attack against a Russian passenger plane in October 2015. Egypt remained in a dire financial position throughout the period studied, with a currency flotation in late 2016 devaluing the Egyptian pound by half.

In the GCC states, Arab Spring protests were also coordinated on social media.[209] All GCC states including Oman subsequently increased violent security activities, especially in the Shia provinces in Saudi Arabia.[210] They also made sudden nationwide gifts, raising the level of state provision in order to mute dissatisfaction. The Gulf states' response to the Arab Spring was as much external as internal. Gulf states were involved in funding and equipping various groups in Syria and Libya, while Saudi Arabia also provided military support to Bahrain during the 2011 protests. The response of GCC states to the pressures of the Arab Spring was therefore dynamic and multifaceted. In Saudi Arabia, this dynamism accelerated after King Salman succeeded King ʿAbdullah after the latter's death in 2014. King Salman's son Muhammad bin Salman, the Crown Prince since June 2017, has undertaken extensive social reforms and championed new economic plans on the one hand, while consolidating his power through mass arrests of elites accused of 'corruption' and the imprisonment of Islamic moderates and activists.

[208] Al-Sisi was re-elected in March 2018.
[209] Philip N. Howard and Muzzamil M. Hussain, 'The Role of Digital Media', in *Democratization and Authoritarianism in the Arab World*, ed. Larry Diamond and Marc F. Plattner (Baltimore: Johns Hopkins University Press, 2014), 186–202.
[210] Toby Matthiesen, *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring That Wasn't* (Stanford, California: Stanford University Press, 2013).

This active foreign policy was reflected in GCC relations with Egypt after the 2011 revolution. Egypt received large loans from Qatar during the Muslim Brotherhood premiership, after detailed coverage of the revolution by Qatari broadcaster Al-Jazeera. After the return of the military to power in Egypt in 2013, financial support came from UAE and Saudi Arabia, rather than Qatar. The latter transfers were partly in return for agreeing to transfer sovereignty of two islands to Saudi Arabia. Leaked recordings from Egyptian politicians indicate that President Al-Sisi was acutely aware of this economic disadvantage, with one remark suggesting that his Gulf partners had "money like rice".[211] However, both domestic and foreign policies of the Gulf states were put under serious pressure by the dramatic collapse in the price of oil in 2014.

Finally, the ostracisation of Qatar in 2017 exacerbated existing tensions between the Gulf states. The boycott was the culmination of a long cycle of dispute and reconciliation between Qatar and its neighbours, including the temporary withdrawal of ambassadors by Saudi Arabia, the UAE, and Bahrain from Doha in 2014. The action split families across the Gulf, leading to accusations of human rights violations. Its general justification was Qatar's support for 'terrorism', defined broadly to include backing for opposition groups elsewhere in the region, such as the Muslim Brotherhood, through such tools as Al-Jazeera. However, more proximate triggers included the increasingly close alignment between Muhammad bin Salman and the crown prince of Abu Dhabi, Muhammad bin Zayed, who long opposed Qatar's links with the Muslim Brotherhood; and the apparent backing, in his visit to Riyadh in May, of US President Donald Trump, who tweeted his support for the quartet the day after the boycott.

The Qatar crisis highlights the shifting political alliances in the region during the period analysed by this thesis, as Egypt and the Gulf states adopted neither their accustomed national roles in the broader Middle East nor maintained regional groupings institutionalised in the post-Cold War environment. Overall, the four intra-regional differences considered in this section are crucial to the four moral manoeuvres detailed in Part 2. Most importantly, they mean that the moral manoeuvre of appropriation performed by these states changes depending on its national context, as the cluster of

[211] David D. Kirkpatrick, 'Leaks Gain Credibility and Potential to Embarrass Egypt's Leaders', *The New York Times*, 12 May 2015, https://perma.cc/CNT5-RYU8.

values around an expansive definition of national security is constructed from both these individual national contexts and the broader patterns across these states noted in this section.

3.3 Cybersecurity governance

The hybrid position of Egypt and the Gulf states in international internet governance, and its subfield, international cybersecurity governance, is one of two reasons for their treatment together as a cybersecurity region in this thesis (the other, a transnational professional community, is analysed in the next chapter). This hybrid position creates contradictions exacerbated by the four moral manoeuvres detailed in Part 2. This section investigates internet governance structures across Egypt and the Gulf states. It uses interviews with cybersecurity professionals who are part of the regional expert community, and the circumstances of the interviews will be detailed in the next chapter.

Internet governance is often described as a binary choice between liberal 'multistakeholder' views, in which government, civil society, and businesses all participate, and authoritarian desires for larger state sovereignty and governmental control of information flows across national borders (cyber sovereignty).[212] In fact, this picture is much more complex, with a variety of approaches to internet governance in both camps.[213] For example, Carr highlights how multistakeholder governance masks the exercise of state power, especially regarding the diminished role of civil society groups in decision-making rather than deliberative fora; what she terms 'power plays'.[214] On the other side of the coin, Cornish has shown how the Chinese approach to digital sovereignty is in fact much more nuanced than simple blanket control.[215]

[212] John E. Savage and Bruce W. McConnell, 'Exploring Multi-Stakeholder Internet Governance' (EastWest Institute, January 2015).
[213] Daniel W. Drezner, 'The Global Governance of the Internet: Bringing the State Back In', *Political Science Quarterly* 119, no. 3 (2004): 477–98; Milton Mueller, Andreas Schmidt, and Brenden Kuerbis, 'Internet Security and Networked Governance in International Relations', *International Studies Review* 15, no. 1 (1 March 2013): 86–104; Hurwitz, 'The Play of States'.
[214] Madeline Carr, 'Power Plays in Global Internet Governance', *Millennium* 43, no. 2 (1 January 2015): 640–59.
[215] Cornish, 'Governing Cyberspace through Constructive Ambiguity'.

Taking this argument further, Raymond and DeNardis have argued that what they call 'multistakeholderism' as a method of global governance is heterogeneous and inchoate, as administrative and regulatory bodies are routinely captured by specific coalitions of both public and private sector actors.[216] Instead, they identify five overlapping 'sets of procedural rules' for internet governance: the liberal ("OECD") view, the authoritarian ("Shanghai Cooperation Organisation") view, a G77 postcolonial view, and technical and corporate views. The argument of this section is that Egypt and the Gulf states take a hybrid position in the simpler bipolar model; however, a similar argument could be made for the same states regarding Raymond and DeNardis' fivefold model, and I identify technocratic and postcolonial rhetoric where it occurs in the following analysis.

The first of these states to engage in international internet governance was Egypt. Egypt participated extensively in early internet governance, presenting itself as a leader in both the Arab world and the developing world more widely. Egyptian delegations were active in both iterations of the World Summit for the Information Society (WSIS), a landmark event in attempts to develop a framework of global internet governance, in 2003 and 2005. President Mubarak gave a keynote speech at the 2003 WSIS summit in Geneva that captured the overall tone of the summit towards new technologies:

> The effects of ICT revolution should not be limited exclusively to achieving economic and developmental gains. It should be extended to strengthening political, social and cultural links among nations; to bringing about world peace based on justice, equality, and respect of international legitimacy; to supporting national efforts towards more freedom, democracy, and respect of human rights. All this should be achieved within a framework that respects national identity and maintains the diversification of particularities, religions, and cultures as key components for cooperation and integration among civilisations.[217]

The domestic context of this speech is important. This was a period of relative freedom in Egypt, where Mubarak was politically and financially able to appeal to several divergent constituencies, although a massive military and security apparatus remained his main lever of power. Domestic and international observers saw expanding possibilities for democratisation in Egypt and

[216] Mark Raymond and Laura DeNardis, 'Multistakeholderism: Anatomy of an Inchoate Global Institution', *International Theory* 7, no. 3 (November 2015): 572–616.
[217] Hosni Mubarak, 'Address of H.E. Mr Mohamed Hosny Mubarak at the World Summit on the Information Society' (International Telecommunication Union, 10 December 2003), https://perma.cc/HPC2-PM8U.

more widely in the Middle East, and so this address mirrored not only the contemporary optimistic view of the internet itself, but also the specific regional context. Moreover, these summits had a long-term discursive effect: human rights would remain part of the broader repertoire of cybersecurity through the rights-based views of government threats to individual privacy and freedom of expression examined in Part 2.

The summit also had a more prosaic long-term influence. It was attended mainly by telecoms ministries, because it was organised by the International Telecommunications Union (ITU), which has provided global telecommunications (originally telegraph) standards since 1865. Egypt originally created a Ministry for Communications and Information Technology (MCIT) in 1999, while between 2000 and 2004 Egypt and all GCC states except for Kuwait created regulatory agencies for telecoms. The responsibility for internet governance and what would become cybersecurity lay with telecoms agencies in the first instance.[218] This meant that early cybersecurity governance was technocratic, focused on aligning standards and enabling business. In this early period, cybersecurity – often under different labels, such as 'information assurance' - was *not* a key site of political contest, partly due to this technocratic appearance. However, this relative lack of political salience, and the core role of telecommunications agencies, would soon be challenged in both Egypt and the GCC, and is explored in Chapter 7.

After WSIS, Egypt continued to participate extensively in bilateral and regulatory activities in internet governance. A delegation from Egypt visited the US Department of Commerce in 2005 to discuss the development of a cybersecurity framework with US government agencies and private sector.[219] In 2008, Cairo hosted the annual summit of the Internet Corporation for Assigned Names and Numbers (ICANN), which has a crucial role in internet governance,[220] as a backup for Kenya's

[218] David Souter and Abiodun Jagun, 'Whose Summit? Whose Information Society? Developing Countries and Civil Society at the World Summit on the Information Society' (APC, 2007).
[219] US Department of Commerce, 'Egypt - Egyptian Cybersecurity Delegation Makes a Consultative Visit', Commercial Law Development Program, 16 September 2005, https://perma.cc/4H5W-XRDF.
[220] ICANN is a controversial organisation, as it was a private company contracted by the US government since its inception in 1998 and was seen as a symbol of US dominance of internet governance. It was finally moved out of US control in 2016.

original offer to host.[221] At this meeting, Tarek Kamel, then telecommunications minister, stressed that this demonstrated Egypt's long-term involvement in internet governance processes, reinforcing its international image as an active member of the global internet governance community.[222]

The ITU also increased its focus on cybersecurity in this period. The ITU first officially included cybersecurity in its remit through the International Multilateral Partnership Against Cyber Threats (IMPACT), created with Malaysian funding and physical location in 2008.[223] The original proposal, made in Texas in 2006, was for a speculative partnership against cyber *terrorism*, joining the international attention and finance provided by the global war on terror.[224] IMPACT was then named the official ITU 'executing arm' for cybersecurity in 2011.

ITU IMPACT was ostensibly separate from the ITU Arab region head office, which was based in Cairo from 2010 and which still saw WSIS as the guide for their role in bringing cybersecurity to the region. An interviewee with extensive experience of the Cairo office emphasised this point, claiming that: "at ITU we are implementing WSIS2. We are building trust and competence. We have a cybersecurity division, and a regional office in the Arab Region, so the Arab region has been aware [of cybersecurity] for 8 years" (I-57). Another interviewee noted that the regional and the head office were significantly different in terms of their technical roles: "You have to distinguish ITU in Geneva from the Regional Office. The latter is capacity building, technical ability is more in the HQ" (I-32). The ITU itself is thus subject to the regionalising processes noted in the first section of this chapter. In this case, the regional branch of the ITU is an intermediary between national and international structures, tasked with implementation of global agreements but without the technical capacity necessary to do so.

The first interviewee above observed that their task was complicated by the turbulent political situation in the Middle East even before the Arab Spring, claiming that "cybersecurity is a priority in the region, but since there is no stability it is difficult" (I-57). Events at the 4th Internet Governance

[221] Rebecca Wanjiku, 'Cairo to Host ICANN Meeting in November', CIO, 20 May 2008, https://perma.cc/NJ8X-ZH9N.
[222] Tarek Kamel, 'Opening Speech ICANN 33rd Meeting Opening Ceremony' (ICANN, 3 November 2008).
[223] Rita Boland, 'Countries Collaborate To Counter Cybercrime', SIGNAL Magazine, 28 July 2008, https://perma.cc/WUY2-TCT2.
[224] Carol Ko, 'Fighting Cyber Terrorism', Computerworld, 17 June 2008, https://perma.cc/6CZF-QG2J.

Forum (IGF) in Sharm Al-Sheikh in 2009 illustrate this point. At the IGF, the OpenNet Initiative (ONI) organised a publicity stand for a book about global censorship, Access Controlled, with a contribution from the cybersecurity scholar Ronald Deibert noted in the previous chapter. However, they were forced to dismantle it by security guards and the IGF officials themselves after a complaint from the Chinese delegation. As Deibert and his colleagues later recounted:

> The now-infamous IGF [ONI] book reception illustrates in one instance the current state of cyberspace contestation. Rather than overt censorship, a member state [China] pressures UN officials at the IGF to remove a poster that alludes to practices (in this case, technical censorship) they would prefer not be mentioned. Meanwhile China is engaging in a forthright campaign to neutralize the IGF, pushing instead for Internet governance to be moved to a more state-exclusive forum. Perhaps not surprisingly, the IGF president seems loath to annoy the member state, perhaps for fear of stirring up yet more animosity toward the IGF. But the quiet show of authority does not go unchallenged - documented by dozens of social-media-enabled activists and attendees, accounts of the event ripple outward to become a media storm.[225]

Deibert's comments illustrate the two competing paradigms of internet governance outlined above, and the limits placed on civil society organisations in both these paradigms. Furthermore, the summary document of this IGF summit signalled the emergence of cybersecurity as a political resource in internet governance, with the anodyne statement that "cybercrime and cybersecurity were noted as key issues by all participants" indicating that the two terms have significant political capital.[226] Differences in interpretation appeared in the detailed discussions, as "in the discussion on cybercrime, it was mentioned that in trying to protect people some were trying to control everything: to gather more data, and to get information about everything that was done online".[227] This contradiction would be widened by the moral manoeuvre of appropriation analysed in Chapter 7.

Although this was a global event, the domestic political situation in Egypt was again a vital backdrop. Sherif Hashem, then head of the Egyptian national cybersecurity response team and an influential figure in regional cybersecurity, spoke at the summit of "the challenges in trying to find the right balance for society and made reference to the Egyptian experience".[228] These guarded

[225] Ronald Deibert et al., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MA: MIT Press, 2011), p.4.
[226] IGF, 'Fourth Meeting of the Internet Governance Forum Chairman's Summary' (Internet Governance Forum, 18 November 2009), p.27.
[227] IGF, p.8.
[228] IGF, p.8.

comments encompassed a significant tightening of the political environment in the years since the first internet summit in 2003. Specifically, large protests in 2005 and on 6 April 2008 had been suppressed brutally by security forces (the 6th April movement, named after this protest, would become a key campaign group after the January 2011 revolution). Hashem's comments show that Egyptian officials were keen to emphasise publicly a 'balance' between cyber sovereignty and the multistakeholder model despite securitised and confrontational domestic politics. Egypt's hybrid position here is both designed for international consumption *and* inculcated by a history of involvement in these governance processes as a non-Western state seeking increased technological opportunities. It embodies the contradictions exacerbated by the intra-governmental struggles detailed in Chapter 7.

In contrast to Egypt, the GCC states were not active internationally in cybersecurity governance until 2011, when the role of social media and information technologies became a hotly contested topic around the Arab Spring. In this politically charged environment, the GCC states are often simply described as opposing the multistakeholder model of internet governance, due to events at the World Congress on Information Technology (WCIT) in December 2012 in Dubai. At this conference, a motion was proposed for the ITU to take responsibility for the naming and numbering functions of the internet from ICANN, as well as implementing various internet security measures through state level regulation. The initial verbal proposal was made by the UAE and supported by Bahrain, Saudi Arabia, Oman, Russia and Iraq, and a written version was signed by the UAE and Saudi Arabia along with Russia, China, Algeria and Sudan.[229] The proposal was widely represented in Western media as a power-grab by authoritarian regimes.[230] It is likely that domestic security concerns partly motivated this proposal, given the theme of the other regulatory standards discussed at the summit.[231] However, this proposal was also framed as a means to 'correct historical

[229] Eli Dourado, 'Behind Closed Doors at the UN's Attempted "Takeover of the Internet"', Ars Technica, 20 December 2012, https://perma.cc/TCG3-2LST.
[230] Elise Ackerman, 'The U.N. Fought The Internet -- And The Internet Won; WCIT Summit In Dubai Ends', Forbes, 14 December 2012, https://perma.cc/GEL3-D7ZM; Rory Cellan-Jones, 'Divisions over Internet Governance Intensify in Dubai', *BBC News*, 10 December 2012, https://perma.cc/9TUB-BS7D.
[231] Elise Ackerman, 'Will A Secretive Summit In Dubai Mark The End Of The Open Internet?', Forbes, 10 December 2012, https://perma.cc/2TY7-DLKL.

imbalances' and 'US dominance', illustrating the relevance of colonial legacies in internet governance more widely and the complexity of the GCC's hybrid position.[232]

Egypt again had a contradictory position at the 2012 WCIT summit, indicating its hybrid position between the two poles of internet governance. Egypt was named on the draft proposal above, but immediately denied that they had supported it. The Egyptian delegation then stated that "Egypt has always supported and will continue to support the concepts of free Internet and has exerted all efforts to develop the Internet and its wide spread among its citizens. Content regulation and censorship are not within the scope of ITRs [International Telecommunications Regulations]."[233] Egypt's inconsistent approach at WCIT mirrors its domestic struggles after the 2011 revolution, as the Morsi government elected earlier in 2012 was increasingly losing control and support, divided between its core Islamist power base and those who espoused the liberal modes of governance captured in the statement above. As will be detailed in Chapter 7, a clear stance on cybersecurity did not appear in Egypt until after the military coup in June 2013.

What is often missed in polarised accounts of WCIT – especially putting the Gulf states simply in the authoritarian camp - is that the ITU is also a site of continual regional contest outside high-profile summits, centrally including the GCC states. Saudi Arabia provides high levels of funding for the ITU – half that of the US, but a similar amount to Russia and China – likely seeking influence over the organisation through these payments.[234] However, throughout 2012 the ITU held negotiations with the Omani government, which agreed to pay $2 million for the first 'Arab Region Cybersecurity Centre' in Muscat, launched officially in March 2013.[235] During this negotiation, the first regional ITU cybersecurity drill was held in Jordan in July 2012, before the Oman centre was established.[236] The next drill was held in October 2013 - but described by the Omani press as the first

[232] Sheetal Kumar, 'Cybersecurity: What's the ITU Got to Do with It?', Global Partners Digital, 9 July 2015, https://perma.cc/BE4P-SBQ5.
[233] Dourado, 'Behind Closed Doors at the UN's Attempted "Takeover of the Internet"'.
[234] Eli Dourado, 'Protecting the Open Internet May Require Defunding the ITU. Here's How to Do It.', Washington Post, 18 September 2013, https://perma.cc/H2WS-2CFP.
[235] ITU, 'ITU-IMPACT Establishes First Cybersecurity Innovation Centre for Arab Region Oman Chosen as New Regional Cyber-Hub', Global Security Mag Online, December 2012, https://perma.cc/MF8F-GZ83.
[236] eGov innovation, 'ITU-IMPACT to Hold Arab Cross-Border Cyber Drill', Enterprise Innovation, 3 July 2012, https://perma.cc/BAY6-YHAX.

one in the region, suggesting that they had been competing with Jordan to attract ITU attention.[237] (Later drills were held in Egypt in 2015 and in Qatar in 2017.) Following the creation of the ITU Regional Centre, Oman was ranked third in the ITU's 2014 'cybersecurity readiness index'.[238] Overall, GCC support of the ITU at WCIT was thus not simply a sudden 'power-grab' for increased surveillance, but a move to support the ITU within a wider context of financial ties and regional competition.

Two other elements of international cybersecurity governance under the United Nations contribute to the hybrid position of Egypt and the GCC states. The first was a Group of Governmental Experts (GGE), created in response to a Russian request for state cooperation in 1998 on information security. Egypt was part of the 4th and 5th GGEs; as detailed in Chapter 2, the latter produced a key report in 2015 stating that offensive actions in cyberspace should obey international law. However, the GGE process itself collapsed in June 2017 over differences in the applicability of international law in cyberspace.[239] In this group, Egypt was directly between the two opposed versions of internet governance promoted by the cyber 'great powers'.

The other international grouping relevant to cybersecurity governance in this region is the GCC itself. However, this involvement has been minimal. The only direct GCC-level contribution in cybersecurity is a joint GCC computer emergency response team (CERT) established in 2006. This lack of cooperation persists despite external encouragement from key security allies. For example, there was a cyber working group with the US in mid-2015,[240] and the US has held annual discussions on cybersecurity with military representatives through a Central Region Cybersecurity conference involving all seven states in this thesis, as well as Lebanon and Afghanistan, from 2010 onwards.[241] The US and its multistakeholder allies do not openly chastise the GCC for their opposition to multistakeholder proposals, as they do for Russia and China, but instead work with

[237] OCERT, 'OCERT Event Details', 23 October 2013, https://perma.cc/XY4F-7ZBN.
[238] ITU Cybersecurity Readiness Index, available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Global_2014_results.pdf.
[239] Maxey, 'Can the Law Restrain Nations in Cyberspace?'
[240] Telecoms Regulatory Authority (Bahrain), 'TRA Heads Bahrain's Delegation to US-GCC Cyber Security Strategic Cooperation Forum', 14 September 2015, https://perma.cc/2JCT-55BA.
[241] Unipath, 'Building a Regional Cyber Partnership', *Unipath* (blog), 20 August 2015, https://perma.cc/Q4S9-G6C5.

them closely on military and security issues including cybersecurity. The extent of US and European support is a fundamental aspect of these states' hybrid position in cybersecurity governance.

Finally, formal GCC-level structures are often token gestures, and the only GCC meeting to explicitly focus on cybersecurity is a good example. The first meeting of the GCC "permanent committee for cybersecurity" (*lajnat al-daʾima lil-ʾamn al-sibrani*) was held in Abu Dhabi in February 2017, by the GCC Police Agency. The UAE media characterised this as a response to "a permanent state of active war in cyberspace with sides that target them electronically, chiefly Iran" (*halatu harb istibaqiyya wa mubashira fi al-fidaʾ al-sibrani maʿa al-jihat alati tastahdifuha ʾiliktrunian, wa ʿala raʾasiha ʾiran*), but also including terrorists such as Islamic State.[242] However, participants merely paid lip service to exchanging expertise and experience and securing information between the GCC. This is an echo of statements made five years earlier in a well-publicised GCC security agreement that also promised information sharing through digital means.[243] However, as detailed above, four months after this meeting, Qatar was ostracised completely by Egypt, Bahrain, Saudi Arabia and the UAE, and the GCC as an organisation became effectively dormant, including in cybersecurity.

In sum, the international landscape in which cybersecurity emerged was one of diverse positions and deep contest, both in the open at key summits and through lower level financial and discursive powers. Although both poles of internet governance were clearly influential in shaping the policies of Egypt and the GCC states, these states did not fit simply into either camp. Instead, Egypt and the Gulf states occupy a hybrid position in international governance, with support from multistakeholder proponents and participation in moves to enhance cyber sovereignty with Russia and China. The extent of struggle over and variation in the values relevant to cybersecurity is plausibly higher in Egypt and the Gulf states than elsewhere because they occupy this hybrid

[242] Staff Report, 'Inʿaqada ʾawl Ijtimaʿa Lilajnat Alkhalijiyyat Lilʾamn Al-Sibrani Bilʾimarat [The Gulf Committee for Cybersecurity Held Its First Meeting in the Emirates]', Al-Khalij, 10 February 2017, https://perma.cc/TZL3-XDEQ.
[243] Habib Toumi, 'GCC Ministers Sign Major Security Agreement', GulfNews, 12 November 2012, https://perma.cc/5S7N-CBN5.

position. This region is thus an important site in which to examine value struggles in cybersecurity, and I argue in Part 2 that these are best captured by the concept of moral manoeuvres.

Chapter 4: Experts

This chapter analyses the professional cybersecurity community in Egypt and the Gulf states. This community is central to the thesis argument, as it is a second key reason for examining Egypt and the Gulf states together as a single region in cybersecurity. It is also the site of the empirical research of this thesis, conducted in 2016 and 2017. This includes interviews with and participant observation of the regional expert community, accessed initially through cybersecurity conferences. All four moral manoeuvres examined by this thesis have expertise at their core, as experts alter issue-specific technical claims and wider values and renegotiate the relationship between them.

This study builds on work in Middle East studies examining the role of professional industries in the region. These works highlight that, especially in the 'late rentier' GCC states, some previously bloated and stereotypically lethargic state bureaucracies become professionalised and represent 'islands of competence' in a redistributive programme of state employment.[244] This is in part due to the exposure of these states to global business practices that privilege technocratic and solution-oriented approaches over political or social debate,[245] and more specifically due to the high levels of education required for the competitive environment of cybersecurity, where there is a longstanding 'skills gap' worldwide.

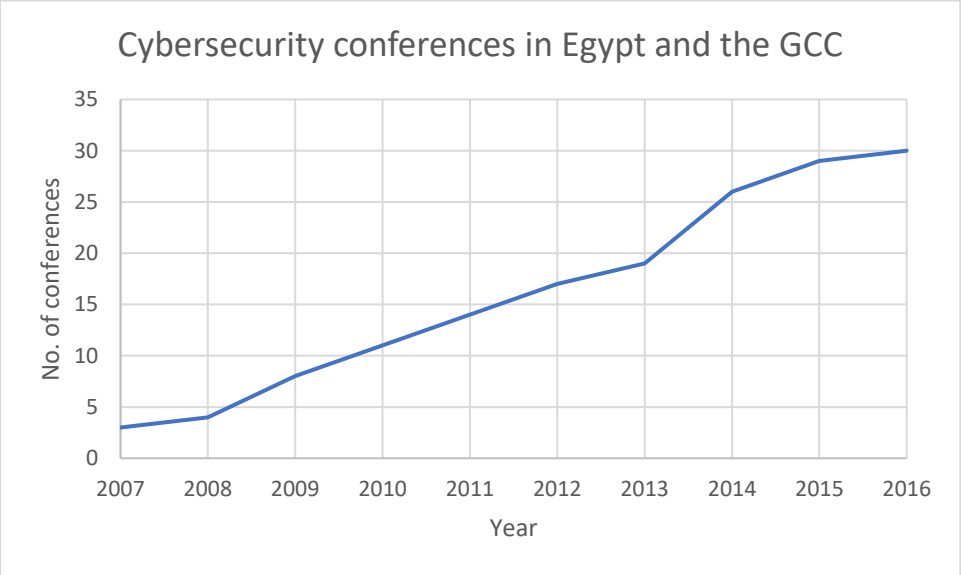
This chapter is structured as follows. The first section details the rise of cybersecurity conferences across Egypt and the Gulf states. The second section provides an overview of the research methods used to access the cybersecurity professional community, and where they appear in the empirical chapters to follow. The third section details the characteristics of the community itself.

[244] Matthew Gray, 'A Theory of "Late Rentierism" in the Arab States of the Gulf', *Center for International and Regional Studies, Georgetown University* Occasional Paper (2011); F. Gregory III Gause, 'Oil and Political Mobilization in Saudi Arabia', in *Saudi Arabia in Transition: Insights on Social, Political, Economic and Religious Change*, ed. Bernard Haykel, Thomas Hegghammer, and Stéphane Lacroix (New York, NY: Cambridge University Press, 2015), p.15.
[245] Steffen Hertog, Giacomo Luciani, and Marc Valeri, eds., *Business Politics in the Middle East* (London: Hurst, 2013).

4.1 Cybersecurity conferences

I accessed the cybersecurity community initially through conferences. Using open sources, I first built a dataset of 165 cybersecurity conferences in Egypt and the Gulf states between 2007 and 2016. The rise in these conferences was substantial, from 2 in 2007 to 28 in 2016, as in Figure 1.

Figure 1: Cybersecurity conferences in Egypt and the GCC



The conferences were selected based on their topic being either 'cybersecurity' or a close cognate such as 'digital security', so larger technology and security conferences were excluded. The conferences include some predominantly hosted by cybersecurity vendors, others organised by professional cybersecurity events companies, and some with support from governments or international organisations. The average attendance, excluding one large outlier (GISEC, with around 4000 attendees) was around 200 people.

Based on structured internet searches, I estimate that this sample covers around 95% of all public conferences.[246] I examine the organisations sponsoring these conferences in detail in Chapter 9. These conferences form the core of both the 'Arab Region' and the 'Middle East' insofar as these terms are used in cybersecurity.

[246] The rise is probably illustrative of world trends, but I do not have space to demonstrate this here.

To understand the role of cybersecurity conferences in creating and maintaining a professional community and expert discourse – a key tenet of the thesis argument - it is instructive to compare cybersecurity conferences to similar situations. In a closely related context, Coleman has argued that 'hacker' conferences embody a particular 'lifeworld', which is brought into being through hackers spending short, intense periods of time together focusing on their common passion. However, Coleman also detected differences in what she called the 'moral economy' of conferences:

> The differences between the American Psychiatric Association annual meetings, where doctors are dressed in suits and mill about during the day at San Francisco's Moscone Center, retiring individually in the evening to a luxury San Francisco high-rise hotel after a nice dinner, and the outdoor festival held by European hackers, where bodies are clothed in tee-shirts and shorts (if that), and many participants can be found sleeping together under the stars of the night, are difficult to deny.[247]

Despite their similar content to the hacker conferences described by Coleman – malware analysis, details of vulnerabilities, stories of famous hacks, and so on – cybersecurity conferences appear to have just as much in common with the drab medical gatherings to which she juxtaposes the hackers' 'ritual celebration'.

Given these differences, another comparison is useful. Scholars have also conducted participant observation at trade fairs for security products (defence technologies, policing equipment, surveillance, and so on). [248] These fairs have a shared genealogy with the cybersecurity conferences I attended, in that some cybersecurity conferences in the Middle East are offshoots of larger defence and security fairs, and defence companies are central figures in the cybersecurity market. In an analysis of a long-running trade fair in the UK, Alexander argues that "these spaces are pivotal in the dissemination, propagation, and reformulation of changing attitudes towards security", as they underpin the "logic of a particular mind-set regarding what it means to consume security as a commodity".[249] I use this theoretical lens to understand the role of cybersecurity conferences in this

[247] Gabriella Coleman, 'The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld', *Anthropological Quarterly* 83, no. 1 (4 March 2010), p.67.
[248] James Alexander, 'Promoting Security Imaginaries: An Analysis of the Market for Everyday Security Solutions' (PhD Thesis, University of Manchester, 2014).
[249] Alexander, p.18.

region as places where cybersecurity is generated, performed, and *reinforced* for the community of professionals who participate in it. They are therefore a central part of the cybersecurity landscape.

One of the methods I employed to access the cybersecurity professional community was participant observation at these conferences. Participant observation has been defined as "immersion in a community, a cohort, a locale, or a cluster of related subject positions".[250] Participant observation is closely associated with a commitment to ethnographic modes of social science research, which "chronicle aspects of lived experience and… place that experience in conversation with prevailing scholarly themes."[251]

Originally, participant observation was for a sustained time at one field site, although an increasingly common method is to use multiple sites, connected in a way that reflects the research design.[252] As Howard describes in his study of digital democracy activists, conferences, although "occurring in sterile hotels… still represent key events full of important social interaction".[253] Despite this potential, conferences are not a traditional ethnographic site, as they are short, happen infrequently, and move between different geographical locations. This has posed a methodological problem for anthropologists, who have conceptualised conferences and similar phenomena in several ways: as 'transitory' sites; as together forming a 'multi-site' ethnography, or as forming one geographically discontinuous site.[254] There are benefits to all three conceptualisations, and I do not distinguish strictly between them. As I argue below, the key point for my purposes is that these conferences do not stand alone but form a cohesive professional community.

I conducted participant observation of seven cybersecurity conferences in Egypt and the Gulf states. I used the conference dataset mentioned above to select the most influential conferences, based on the spread of their attendees, their reputation in the community, their organising bodies, the

[250] Edward Schatz, ed., *Political Ethnography: What Immersion Contributes to the Study of Power* (Chicago: University of Chicago Press, 2009), p.5.
[251] Lisa Wedeen, 'Reflections on Ethnographic Work in Political Science', *Annual Review of Political Science* 13, no. 1 (1 May 2010), p.257.
[252] Jan Kubik, 'Ethnography of Politics', in *Political Ethnography: What Immersion Contributes to the Study of Power*, ed. Edward Schatz (Chicago: University of Chicago Press, 2009).
[253] Philip N. Howard, 'Network Ethnography and the Hypermedia Organization: New Media, New Organizations, New Methods', *New Media & Society* 4, no. 4 (1 December 2002), p.561.
[254] Mark-Anthony Falzon, ed., *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research* (London: Routledge, 2009).

length of time they had run for, and their presence in different states across the region. I participated in these conferences in Egypt, UAE, Oman, Saudi Arabia, Qatar and Bahrain in 2016 and early 2017. More prosaic research characteristics such as budget and time constraints also affected my choice. The seven conferences are in Table 1.

Table 1: Participant observation in cybersecurity conferences

Name	Location	Date attended	Years held (to date)	Organising body
ITU Arab Region Cybersecurity Summit (ARCS2016)	Sharm Al-Sheikh	October 2016	2014-2017	Egypt National Telecommunications Regulatory Authority (NTRA), International Telecommunications Union (ITU).
FIRST Middle East (FIRST2016)	Sharm Al-Sheikh	November 2016	2016	Egyptian NTRA, FIRST (non-profit association of CERTs)
Cairo Security Camp (CSC2016)	Cairo	November 2016	2010-2017	Bluekaizen (cybersecurity company)
RSA MENA (RSAAD2016)	Abu Dhabi	November 2016	2012-2017	RSA (cybersecurity and events company)
Cybersecurity for Critical Assets MENA (CSCA2016)	Dubai	November 2016	2015-2016	Qatalyst Global (cybersecurity events company)
Middle East Cybersecurity (MECS2017)	Riyadh	April 2017	2015-2017	Nispana (events company)
ITU Arab Region Cybersecurity Summit (ARCS2017)	Muscat	November 2017	As above	Oman Information Technology Authority (ITA), ITU.

As a delegate at these conferences (with a badge accurately labelling me as a Research Affiliate at the Cyber Studies Programme, University of Oxford), I participated as a cybersecurity professional. My profile as a white male and a native English speaker with working Arabic proficiency was an important part of participant observation. I was quickly put into specific

categories – consultant, guest speaker – by my interlocutors, and treated in a way which would have changed had my gender, ethnicity, or language been different. As a recognisable label with extensive social and academic associations, 'Oxford' both increased my acceptance and made it suspicious. As one interviewee mentioned, pointing out Oxford University's connection to the UK intelligence community, "they don't know who you are, you come from a country with a bad history in these things, they don't know what you will do with the information" (I-36).

My interviews indicate that conference attendees do not have a single view on the character, purpose, or utility of conferences. On one hand, for some interviewees conferences were mainly profit-making exercises. One interviewee told me that "I start to sense that everything is commercialised more, and conferences become a business. It is a devaluation of conferences or workshops." (I-53). Another specifically named one of the conferences I attended as a commercialised environment, saying that "there is a market for infosec events, RSA and GISEC, it's maybe saturated. It helps in awareness raising." (I-39). It is worth noting that RSA Abu Dhabi is an offshoot of a high-profile US conference attracting thousands, and it inherits several theatrical characteristics including large auditoriums, walk-on music and dimmed lights for keynote speakers, and extensive awards speeches at the close.

Other interviewees recognised the commercial side to conferences but claimed that they were nonetheless valuable. One interviewee said that "lots of them are commercial, living in their own shell, the firewall guy trying to sell his firewall. But I don't mind having them, because at least people get interested in it." (I-38). Another said that "It's good for sales of course, but also helping to learn from others' experiences." (I-17). Another said that they attended even though they recognised the problems, saying that "these conferences are generally all vendors, it's hard to find an actual delegate to talk to. But there are a lot of good ideas, and I do go to a lot of them." (I-11).

My experience at these conferences indicates that cybersecurity professionals move frequently within Egypt and the GCC states, forming a single professional community. As one interviewee said, 'at all the events you go to… you keep stumbling across the same people' (I-42). This networking purpose was clear to other interviewees. One remarked that "it is a networking event rather than a learning event. 80% of them are networking" (I-51), while another said that "it is

important to be there because all our local stakeholders are there. They attend the conferences and we can engage with them there" (I-36). Finally, one interviewee associated conferences with the projection of a specific international image: "conferences are surprisingly important, and do get seniors in, and it's a pride thing – each country wants to show that they can get the big companies there, so they are important and thriving" (I-41).

This community also saw speaking at conferences as a worthwhile use of their time. On one hand, speakers could be too famous: "you get these cybersecurity superstars, and they are run by an event company, it's cheesy theatre. They want people to turn up and pay 100K." (I-44). On the other hand, an interviewee saw it as both a strategic advantage and professional duty, saying that: "when you speak you are exposed to more job opportunities, they come to you, you can change jobs. Also I want to give back something: it is all giving and taking, like this interview! I speak to be on an expert level in the industry." (I-51).

If, as the interviewee above suggests, conference speakers are on an 'expert level', it is worth examining how this expert performance takes place. The fundamental division in the physical space of conferences is between the outer layer of company-branded booths and the inner layer of presentation rooms; in other words, between a space for commerce (the trade stands) and a space for knowledge (the central auditorium and breakout rooms). Speakers conform to this division in their on-stage performance, disclaiming any "sales pitch" when delivering talks, even about their product, although this is often undermined by the company copyright of their slides. The conference space is therefore an explicit acknowledgement and simultaneous separation of both the myriad commercial incentives for conference organizers, hosts, speakers, and attendees at the outer layer, *and* their claims to possess an independent and unbiased expert knowledge at the inner layer.

Crucially, the separation of knowledge and commerce shapes cybersecurity expertise by inscribing the ability to alter their performance between these spaces—to shift repertoire—as a core skill for cybersecurity experts. The same people deliver their independent expert judgement on stage, and then an unashamedly partisan view of their superior product after returning to their booth. I do not mean to imply that either is incorrect, or that to do both is necessarily hypocritical, but that this duality is imposed by the separation of the conference space itself. Consequently, cybersecurity

expertise is essentially flexible, with several registers and the capacity for context-based improvisation. The ambiguity of cybersecurity expertise is not simply a discursive or conceptual characteristic but is reinforced by the physical act of speaking at cybersecurity conferences. Other sources of this ambiguity are explored in the last section of this chapter and in Chapter 5.

4.2 Other forms of access

In this section, I provide the details of three other methods I used to access the cybersecurity professional community in Egypt and the Gulf states, in addition to the participant observation above. Two of these methods are common qualitative techniques - discourse analysis and interviews – while the third is a further method I term 'investigation'. I treat the three methods in turn below. The combination of methods and data sources provides a more comprehensive view of the cybersecurity professional community, and thus a greater understanding of its ambiguous expert discourse.

Like participant observation, all three methods in this section are qualitative. Klotz and Prakash define qualitative methods for IR as starting from the premise that "language as a form of observable behaviour", and so qualitative social science is fundamentally "linked to meaning".[255] This highlights that what Geertz terms 'thick' description – consciously detailed observation rather than seeking to abstract or capture a central essence - is a central element of the analysis.[256] On another spectrum, this analysis lies further towards an 'interpretivist' rather than a 'positivist' research design.[257] Interpretivist research acknowledges and incorporates the researcher's position and interaction with research subjects into the process of data collection.[258] However, interpretivist and positivist research designs cannot be neatly divided, and my investigation of cybersecurity in Egypt and the Gulf states includes elements of both, aiming towards what Glynos and Howarth call

[255] A. Klotz and D. Prakash, eds., *Qualitative Methods in International Relations: A Pluralist Guide* (Basingstoke England; New York: Palgrave Macmillan, 2008), pp.1,3.
[256] Clifford Geertz, *The Interpretation Of Cultures* (New York: Basic Books, 1977).
[257] Dvora Yanow and Peregrine Schwartz-Shea, *Interpretation and Method: Empirical Research Methods and the Interpretive Turn* (London; New York: Routledge, 2013).
[258] Patrick Thaddeus Jackson, *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics* (London; New York: Routledge, 2010).

an overall "logic of critical explanation".[259] This approach has affinities with the research methods developed by critical security studies, which I highlight in the following discussion.[260]

4.2.1 Discourse analysis

Discourses are systems of signification that are productive of various entities (including people, places and objects), changeable and historically contingent.[261] There are four discourses I analyse in this thesis, only one of which is linked to the conferences above. I distinguish these discourses because the structure and content of the texts in these corpora is substantially different and bears little similarity to the others apart from the label 'cybersecurity'. In other words, these texts are produced in different ways by different actors, and so I took the methodological decision to analyse them separately, identifying detailed features rather than broader patterns across the whole discourse of cybersecurity in Egypt and the Gulf states. The four discourses are in Table 2.

Table 2: Cybersecurity discourses in Egypt and the GCC

Discourse	Text type	Text source	Thesis location
Government	Legal	National cybercrime laws, international agreements	Chapter 7
	Strategic	National cybersecurity strategies	Chapter 7
Private sector	Incident	Technical incident reports, media reports on these incidents	Chapters 5, 6
	Publicity	Public statements on misuse and sales policies, leaked documents	Chapter 8

[259] Bent Flyvbjerg, *Making Social Science Matter: Why Social Inquiry Fails and How It Can Succeed Again* (Cambridge: Cambridge University Press, 2011); Jason Glynos and David Howarth, *Logics of Critical Explanation in Social and Political Theory* (London; New York: Routledge, 2007).
[260] Karin M. Fierke, *Critical Approaches to International Security* (Cambridge: Polity Press, 2007); Laura J. Shepherd, ed., *Critical Approaches to Security* (London; New York: Routledge, 2012).
[261] Jennifer Milliken, 'The Study of Discourse in International Relations: A Critique of Research and Methods', *European Journal of International Relations* 5, no. 2 (1 June 1999): 225–54.

The distinction used by many discourse analysts between 'official' and 'non-official' or 'semi-official' texts is replaced here by one between government and private sector. Government discourse is, as the name suggests, explicitly identified with a government institution. In turn, government discourse is either legal or strategic: the former includes cybersecurity laws and regulations, as well as international agreements, while the latter include cybersecurity strategies and policies. In contrast, private sector discourse is explicitly identified with a private company, although potentially written by the same person, as experts cross regularly between public and private sectors. While the first private discourse – incidents – is fairly self-explanatory, in that it includes technical reports about cybersecurity incidents and media reports based on those incidents, the other category requires slightly more explication.

In the 'publicity' category, I collected public statements from non-official sources, including news reports, interviews, and public statements released after publicity surrounding human rights violations associated with cybersecurity technologies. 57 non-duplicate documents were retrieved, each including multiple statements. Private statements were retrieved from over a million emails released on the website Wikileaks in 2015 after a leak from Hacking Team, and a similar leak from FinFisher in 2014 with product and customer details. I narrowed the texts selected from the Hacking Team leak by searches for references to 'moral', 'ethics', 'ethical', 'human rights', and 'Wassenaar', with 38 email chains (with approximately 10-50 individual emails in each) containing significant discussion. While I cite texts taken from news reports in the same way news reports are cited generally in this thesis, I cite the Hacking Team texts as an archive, by referring to the reference number given to the email by Wikileaks, with a list of the emails included as a separate item in the bibliography.

There are additional ethical issues associated with the use of leaked emails, as these are statements not intended for the public domain made by people who are still professionally active. On one hand, they are an invaluable source of moral debate within the company, as I show in Chapter 8, because they remove a layer of deliberate presentation from the text (of course, there remain other layers of artifice). On the other, there is the possibility that my analysis of these emails, many of which have not been interrogated before, could reveal information that has a damaging impact on its

author. To address this issue, I do not attribute quotations from this archive to individuals, and only present in the thesis email sections that are directly relevant to the research question.

The method of discourse analysis involves three elements: text selection, coding, and analysis.[262] 'Text' here has a broad meaning, as it can be anything involved in a system of signification; images, videos, and objects are often part of linguistic or semiotic systems (as indicated in the discussion of materiality in Chapter 2). 'Coding' is a specialised term with a different meaning here to that elsewhere in the thesis, where it refers to computer code. Discourse analysts use 'coding' to mean the analytical structure applied by the researcher to the texts, i.e. which elements of the text refer to which aspects of the research question. Coding structures can be generated prior to or after engagement with the text (the latter known as 'in vivo').[263] I generated analytical categories in vivo and performed all coding on the qualitative analysis software MaxQDA. Finally, discourse analysis techniques lie on a spectrum between quantitative and qualitative; the former counts machine-identifiable syntactic structures in large quantities of text, while the latter requires semantic engagement with smaller quantities of text by the researcher, often summarised by displaying significant quotations. My approach strongly leans towards the latter end of the spectrum.

For ease of exposition, in this thesis I refer to the incident discourse above as ' the ambiguous expert discourse', with these ambiguities discussed in Chapter 5 as a generic 'organisational' conception of cybersecurity. The other three discourses build on this organisational conception, and each form part of a moral manoeuvre. The two government discourses above are part of the moral manoeuvre of appropriation, as cybersecurity strategies enhance ambiguities already present in the expert discourse, and laws appropriate this conception of cybersecurity. The publicity discourse is part of the moral manoeuvre of manipulation performed by international surveillance suppliers, treated in Chapter 8.

[262] Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (New York: Routledge, 2006), pp.65-82.
[263] Udo Kuckartz, *Qualitative Text Analysis* (Los Angeles: SAGE, 2014), p.134.

4.2.2 Interviews

Another method I used to access the cybersecurity professional community was interviews with individuals within that community, used throughout Part 2. The following discussion addresses five key aspects of interviewing as a qualitative social science method: selection procedure, interview structure and performance, ethical issues and anonymity, and use of interview data.

Interviews were obtained in two ways. The first method was to approach organizers and speakers at cybersecurity conferences. To identify influential individuals in the cybersecurity professional community, I created a dataset of invited speakers at the professional cybersecurity conferences above, including the number and frequency of conferences attended by these speakers. The total number of speakers was 1177. The rationale behind this step was that conference speakers are more influential than other professionals due to their self-selection as an authoritative voice by the community, as indicated by the quotations in the discussion on conferences above. The limitation of this step was that the influence of a conference speaker is public, rather than private, and there may be hidden lines of influence not captured using this method. Within this dataset, I identified the most frequent speakers, defined at speaking in at least three conferences and across more than one conference series. The rationale was that such speakers are more influential than those who speak rarely and are more likely to be part of the regional cybersecurity community due to their greater participation. The total number of such speakers was 96, from which I conducted 24 interviews.

The second selection method was through snowball sampling: asking for recommendations from other individuals I had interviewed. This method produced 32 further interviews, with a total number of 57 (the recommended number of interviews for interpretivist social science varies considerably, but generally ranges between 10 and 60).[264] It also added weight to the first selection process above, as interviewees often recommended others who were also frequent conference speakers. Interviews were conducted in 2016 and 2017 in London, on four fieldwork trips in January 2016, July and August 2016, October and November 2016, and March and April 2017, or by Skype and email if a face-to-face meeting was not possible. Interview dates and locations, along with

[264] Rosalind Edwards and Janet Holland, *What Is Qualitative Interviewing?* (London: Bloomsbury, 2013).

anonymised interviewee characteristics, are presented in Table 3. Further details on the demographic characteristics of cybersecurity professionals are explored in the last section of this chapter.

Table 3: Interviews

Interviewee	Current affiliation	Date	Previous affiliation	Date	Country of origin	Interview location	Date
1	Public - cybersecurity	2006-2016	Public - cybersecurity	2012-2016	Oman	Sharm El Sheikh	03/11/2016
2	Private - finance	2009-2016	Private - IT	2008-2009	Pakistan	Dubai	21/11/2016
3	Private - defence	2014-2016	Private - energy	1998-2014	Pakistan	Abu Dhabi	15/11/2016
4	Public - cybersecurity	2007-2016	Private - leisure	2006-2006	Qatar	Doha	09/04/2017
5	Public - IT	2012-2016	Private - finance	2010-2012	Oman	Muscat	14/08/2016
6	Private - consultancy	2015-2016	Public - cybersecurity	2007-2015	Egypt	Sharm El Sheikh	03/11/2016
7	Private - cybersecurity	2012-2016	Private - energy	2009-2012	France	Abu Dhabi	16/11/2016
8	Public - cybersecurity	2014-2016	Public - cybersecurity	2008-2014	India	Email	22/11/2016
9	Private - IT	2009-2016	Private - IT	2005-2008	France	London	16/08/2016
10	Public - cybersecurity	2011-2016	Private - academia	2013-2016	KSA	Email	04/04/2017
11	Private - defence	2006-2016			UK	Abu Dhabi	15/11/2016
12	Private - IT	2015-2016	Public - cybersecurity	2007-2015	Egypt	Doha	10/04/2017
13	Private - cybersecurity	2015-2016	Private - cybersecurity	2013-2015	UK	Abu Dhabi	14/11/2016
14	Private - consultancy	2016-2016	Private - academia	2014-2016	Switzerland	Email	06/04/2017
15	Private - cybersecurity	2015-2016	Private - IT	2001-2015	USA	Abu Dhabi	14/11/2016
16	Public - infrastructure	2016-2016	Private - IT	2013-2016	UK	Dubai	23/11/2016
17	Private - telecoms	2006-2016			Egypt	Dubai	23/11/2016
18	Private - IT	1998-2016	Private - consultancy		Egypt	Sharm El Sheikh	03/11/2016
19	Public - IT	2005-2016	Private - telecoms	2000-2004	Qatar	Email	12/04/2017
20	Private - consultancy	2016-2016	Private - academia	2014-2016	USA	Abu Dhabi	15/11/2016
21	Private - cybersecurity	2013-2016	Private - finance	2010-2013	Egypt	Abu Dhabi	16/11/2016
22	Public - security	2015-2016	Public - security	2013-2015	KSA	Email	20/05/2017
23	Private - cybersecurity	2013-2016	Public - defence	2005-2011	UK	Email	07/06/2017
24	Public - cybersecurity	2009-2016	Public - telecoms	2004-2013	Egypt	Cairo	09/11/2016
25	Private - defence	2006-2016			UK	London	09/06/2016
26	Public - cybersecurity	2010-2016			UAE	Abu Dhabi	16/11/2016
27	Private - finance	2011-2016	Private - leisure	2008-2011	Singapore	Muscat	16/08/2016
28	Private - energy	2013-2016	Private - consultancy	2004-2010	India	Muscat	14/08/2016
29	Private - cybersecurity	2010-2017	Private - consultancy	2006-2010	UK	London	13/12/2016
30	Private - defence				UK	London	12/09/2016
31	Private - consultancy	2008-2016	Private - IT	1995-2008	India	Manama	23/03/2017
32	Public - international	2004-2016	Public - telecoms	2004-2004	Syria	Skype	15/06/2017
33	Private - consultancy	2016-2016	Public - Foreign Min.		UK	Manama	23/03/2017
34	Public - IT	2014-2016	Private - finance	2012-2014	Oman	Muscat	14/08/2016
35	Private - telecoms	2002-2016			Egypt	Cairo	09/11/2016
36	Public - IT	2014-2016	Private - cybersecurity	2008-2014	France	Doha	09/04/2017
37	Public - security	2014-2016	Private - IT	2005-2011	UK	Riyadh	30/03/2017
38	Private - telecoms	2014-2016	Private - IT	2009-2013	Pakistan	Dubai	24/11/2016
39	Public - Dept. Trade	2016-2016	Public - Foreign Min.		UK	London	22/09/2016
40	Private - academia	2016-2016	Private - finance	2010-2016	UAE	Skype	08/12/2016
41	Private - defence				UK	Gloucester	22/08/2016
42	Private - consultancy	2016-2016	Private - defence	2006-2016	UK	London	15/04/2016
43	Private - consultancy	2008-2016	Public - defence		UK	Dubai	24/11/2016
44	Private - cybersecurity	2013-2016	Public - security	2000-2013	UK	London	24/06/2016
45	Public - Foreign Min.	2014-2016	Private - cybersecurity	2011-2012	UK	London	23/06/2016
46	Public - Security	2008-2016	Public - defence	1989-2012	UK	Muscat	15/08/2016
47	Private - cybersecurity		Public - defence		UK	London	19/08/2016
48	Private - cybersecurity	2011-2016			Pakistan	Dubai	23/11/2016
49	Private - consultancy	2016-2016	Private - defence	2005-2016	UK	London	12/05/2016
50	Private - cybersecurity	2016-2016	Private - IT	2007-2016	Pakistan	Riyadh	05/04/2017
51	Public - Min. Justice	2009-2016	Private - IT	2006-2009	Somalia	Riyadh	04/04/2017
52	Private - finance	2013-2016	Private - IT	2012-2013	Bahrain	Manama	23/03/2017
53	Public - cybersecurity	2011-2016			Pakistan	Doha	12/04/2017
54	Public - cybersecurity				UAE	Dubai	24/11/2016
55	Public - telecoms	2016-2016	Private - telecoms	2012-2016	Bahrain	Manama	21/03/2017
56	Public - international				Egypt	Email	26/01/2018
57	Public - international				Lebanon	Muscat	21/11/2017

The methodological conception of interviewing I adopted, in line with the qualitative social science methodology outlined above, holds that the generation of knowledge through interviewing is a process of mutual performance. This performance is based on a wide range of factors, including the circumstances of the interview, the body language and personal responses to the interviewer of the interviewee, and their interests and goals. Given this conception, the most suitable interview formats are semi-structured or unstructured interviews: both allow the interviewee to follow their own thread, although semi-structured interviews also have a list of planned prompts or questions which can be used to the degree judged appropriate by the interviewer, as well as 'floating prompts' which are drawn from the interviewee's remarks.[265]

I used semi-structured, open interviews, which generally lasted between an hour and two hours, and which began with the same script and prompts. I began by asking the interviewee what they thought were the most important aspects of the emergence of cybersecurity in the region; sometimes they mentioned the topics on my script, and sometimes they did not. If the conversation topic went off cybersecurity completely, I attempted to bring it back, but had to do so rarely. 43 of the 57 interviews are directly quoted in this thesis, although they all informed my overall view of the regional professional community. Interviews were held in English, as technical terms are often in English (a cultural dominance noted by many interviewees). Some differences in Arabic (for example, the root and origin of 'cyber' and its affiliates) will be highlighted in later chapters. I, like all scholars, brought not only my conscious reasons for research to interviews, but also the gamut of other less conscious aspects captured by the concept of 'positionality'.[266] As Holmwood notes, scholarly research of this kind should therefore demonstrate a humility and willingness to engage with differing views.[267]

[265] Beth L. Leech, 'Asking Questions: Techniques for Semistructured Interviews', *Political Science & Politics* 35, no. 4 (December 2002): 665–68.
[266] Jack L. Amoureux and Brent J. Steele, eds., *Reflexivity and International Relations: Positionality, Critique, and Practice* (London; New York: Routledge, 2015).
[267] John Holmwood, 'The Challenge of Global Social Inquiry', *Sociological Research Online* 14(4)13 (31 August 2009).

Interviews can be very unreliable sources.[268] The role of interviews, in this thesis, is not to record unambiguous facts about the emergence of cybersecurity in the region; instead, it is to allow cybersecurity professionals an alternative space in which to perform as cybersecurity experts, away from the public environment of conferences. The main disadvantages of interview data are circumstantial constraints and partial, guarded or misleading responses, as well as lack of or changes in memory. Understanding interview as performance prevents unrealistic expectations, although the danger of deliberate misleading information cannot be entirely avoided.

Finally, interview ethics and anonymity were central to this method. Consent to interviews was obtained via email if possible, in which I outlined the purpose of the research project ('to examine cybersecurity in Egypt and the Gulf states'), the role of interviews and the use of data. If this was not possible, I obtained verbal consent prior to the interview based on the same information.[269] My chosen method of accommodating sensitive information was to anonymise all interviewees in any published text to the degree requested by the interviewee: for example, as "cybersecurity professional in Egypt" or "government employee in Bahrain". Interviewees were given the choice of written or electronically recorded notes and were informed that at any point they could terminate the interview or move to an 'off the record' position. Interviews took place in locations chosen by the interviewee, often in public cafes, office buildings, or conference hotels. All identifiable data was stored on an encrypted hard drive, and multiple levels of encryption and obfuscation were used for devices taken on fieldwork to store interview transcripts. I often used hand-written notes because phones and digital recording devices are easily compromised by third parties (as will become apparent later in the thesis), and cybersecurity experts were especially uncomfortable in having an unknown device on the table throughout the interview.

[268] Aaron Wildavsky, 'The Open-Ended, Semistructured Interview: An (Almost) Operational Guide', in *Craftways: On the Organization of Scholarly Work*, by Aaron Wildavsky (New Brunswick, N.J: Transaction Publishers, 1993), p.62.

[269] The interview procedure was approved by the DPIR Departmental Research Ethics Committee (DREC), with the reference SSH_DPIR_C1A_15_003 on 20 November 2015.

4.2.3 Investigation

So far, I have provided an overview of three familiar qualitative social science methods: discourse analysis, interviews, and participant observation. It is a noticeable aspect of research in security studies that "the security practices we study… are often methods themselves".[270] In this case, the practices of cybersecurity professionals are themselves methods of finding out information about the world, just as the three methods above are ways of finding out about the practices of cybersecurity professionals. Given this dual relationship, there is "extensive circulation between the practitioners of 'academic' methods and those of 'security' methods".[271]

I take advantage of this circulation and use a security method – that of investigation – for academic purposes. By investigation, I mean a structured, focused way of answering a specific question using all available resources, as the term is used in national security agencies and police forces. Another way of describing this model is as an investigation of 'open source intelligence', including structured searches of all databases available to the University of Oxford, and online more widely. The purpose of labelling this method 'investigation' is to highlight the similarity between what I do as a social scientist *investigating* experts, and what those experts do themselves. These are not different kinds of knowledge supporting a firm distinction between the theoretician and the practitioner; but merely used in different contexts, with different aims and constraints.

I used investigation where I treated the texts in question *not* as part of the cybersecurity discourse itself (considered in discourse analysis above), but as a relatively non-discursive source of facts. These facts are of course contingent, context-dependent and shaped by many factors outside cybersecurity, but that is not my focus; such influences are therefore 'bracketed' in this thesis. Their credibility must be weighed against the rest of the data gathered, and against my own experience and interaction with cybersecurity professionals above, both of which provide an extra layer of assessment. This is very similar to investigation in non-academic areas, where credibility and

[270] Claudia Aradau et al., eds., *Critical Security Methods: New Frameworks for Analysis* (London; New York: Routledge, 2014), p.5.
[271] Aradau et al., p.5.

reliability must be weighed using an analyst's expertise as well as structured guidance. Table 4 provides a brief list of the topics selected, and their place in the thesis and the argument.

Table 4: Topics of investigation

Topic	Thesis location
Information on Wassenaar Arrangement and its implementation	Chapters 6, 8
Development of cybersecurity institutions in Egypt and Gulf states	Chapter 7
Information on human rights violations (structured searches on HR NGO websites)	Chapter 7
Information on exporting bodies in the US and UK	Chapter 8
Information on cybersecurity companies (structured searches on ProQuest, Nexis)	Chapters 8, 9

In sum, I used several methods to expand my access to the professional cybersecurity community in Egypt and the Gulf states, as well as participant observation at cybersecurity conferences. For ease of exposition, these methods are integrated in the empirical chapters of this thesis, although I highlight the use of specific methods as and when they are central to the argument.

4.3 Community characteristics

In this section I outline the contours and characteristics of the cybersecurity professional community in Egypt and the Gulf states. I draw on interviews and publicly available data about the most frequent speakers at cybersecurity conferences. This section argues that the ambiguity of the cybersecurity professional discourse is not only inherited through the broader genealogy of cybersecurity but is also a result of the complexity of the expert identities present in this regional community.

4.3.1 Qualifications

Who counts as a cybersecurity expert? In many professional or skilled occupations, community boundaries are determined by formal markers, such as membership in professional associations, standards, or qualifications. I examine each of these in turn, arguing that cybersecurity expertise in Egypt and the Gulf states is not a simple matter of exams or certificates, but a complex product of age, experience, status, and education.

There are international professional associations for cybersecurity with chapters in most countries. Interviewees in Egypt, Oman, and Bahrain mentioned the local chapters of ISACA, a professional association for IT governance, which administers the popular Certified Information Risk Manager (CISM) qualification. Others mentioned the Information Systems Security Association (ISSA), which is also active in Bahrain, Saudi Arabia, Egypt, and Qatar. Finally, OWASP, or Open Web Application Security Project, which produces a popular list of website vulnerabilities, was also occasionally mentioned by interviewees. Although these professional associations create a space for cybersecurity professionals to interact, interviewees did not see them as a condition of entry into the community and many cybersecurity professionals are not members of such organisations.

There are also national and international cybersecurity standards produced by organisations such as the US National Institute for Science and Technology (the NIST framework), the International Standards Organisation (the ISO27000 series), and the UAE National Electronic Security Authority (based on the NIST framework). Surveys suggest that implementation of these standards is uneven in the GCC (comparable data is not available for Egypt).[272] Specifically, a survey of ISO27001 in Saudi Arabia in 2014 suggested that standards were low on security professionals' priorities, below personnel issues like training, expertise, or salary, and organisational ones such as

[272] BI-ME, 'Cisco and GBM Unveil Latest UAE Security Research at GITEX 2014', 14 October 2014, https://perma.cc/EU3X-Z9W3; CISCO, 'Cisco and GBM Outline Key Steps for Digitization to Help Middle East Organizations Become IoT Ready', 19 October 2015, https://perma.cc/UZA5-5ACM.

management involvement.[273] Finally, competition between standards, for example in the UAE between Abu Dhabi-based NESA and Dubai's separate Information Security Regulations (ISR), also prevents one particular standard becoming an indicator of cybersecurity expertise. Overall, adherence to or expertise in specific cybersecurity standards was not a defining feature of cybersecurity expertise in the region.

Expert communities can also be identified through education and qualifications. Of the 74 (of 96 total) most-frequent speakers at cybersecurity conferences whose education was publicly accessible, 14 had a PhD and 38 had a MSc as their terminal degree. 22 were educated to a university level in the UK or US, and 31 had a cybersecurity certification such as CISSP (Certified Information Systems Security Professional). Some interviewees saw these qualifications as a means to portray expertise to other professionals. For example, one interviewee said that:

> I did my CISP in 2006, and MSc in 2008. I decided I want to be a speaker, I attended and said to my friend I wanted to speak, I got him to take a picture with me at the podium. He said you can't be, these people work at HP, at CISCO, big companies. Then I became a speaker and I was paid 60000 SAR [Saudi riyals] to speak! I did certificate after certificate after certificate, and thought what else can I do? I can't do more certificates because I will get bored. I need to remain in the industry, and have the label of expert, so I said I wanted to be a speaker (I-51).

Another interviewee saw qualifications as an attempt to both raise the salience of cybersecurity overall and to promote their expertise. This interviewee said that "security professionals try to grow the industry, certifications and suchlike are there to give them credibility. Because they left school and didn't get a degree, so it gives them something to prove their value - there's an agenda." (I-27). In contrast to the first interviewee, this interviewee was sceptical of the worth of cybersecurity qualifications, seeing individuals with such qualifications as having their own 'agenda'. Therefore, qualifications are also not a guaranteed indicator of cybersecurity expertise, given the wide range of available qualifications and the scepticism of some about their real value.

If common markers of professional communities were not prevalent in Egypt and the Gulf states, how were the boundaries of the cybersecurity professional community defined? The first

[273] Khalid I. Alshitri and Abdulmohsen N. Abanumy, 'Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia', in *2014 International Conference on Information Science Applications (ICISA)*, 2014, 1–4.

interviewee above provided one indication: that the identity of a cybersecurity expert comes not from associations, standards or qualifications, but from experience and employment by recognised organisations. Specifically, for this interviewee legitimation by 'big companies' like HP and CISCO was a key marker of a cybersecurity expert. Specialised cybersecurity companies also confer legitimacy, and I examine how these companies train and recruit cybersecurity experts in Chapter 9.

While corporate experience was an uncontroversial source of legitimacy for cybersecurity experts, the impact of government experience was more complicated. One interviewee, a Qatari former military official, described how their military experience could be detrimental to improving cybersecurity:

> You can't put a uniform on cyber… I will always have this military mindset which influences my behaviour, it is now part of my genes. If cyber is in uniform people will always think of apprehension, legality, with this mindset you can't transform the nation to smart or digital (I-4).

Here, they suggest that the military habitus is unsuited to cybersecurity because it presents an (overly) securitised version of cybersecurity itself for the general public. A similar problem was noted by a UK national, who complained that cybersecurity in the region was permeated with "RAF wing commander types" (I-42). This phrase is interesting, as it pinpoints not merely the ambiguity of military involvement in the cybersecurity professional community, but also tensions within the military, implying that older officers are unsuited to the technological demands of cybersecurity.

However, military and martial logics are deeply embedded in cybersecurity itself, as noted in Chapter 2 and apparent at the conferences I attended. At the 2017 Arab Regional Cybersecurity Conference, a speaker with no military background spoke for an hour on cyber threats with the manner of a military commander. Addressing the audience in a stern tone, they repeatedly claimed that "we are soldiers, all of us here" (ARCC2017). Similarly, martial themes are an essential advertisement and quasi-metaphorical motivational resource for promoting the profession itself. The recruitment slogan of Raytheon, a key participant in cybersecurity in the region, asks candidates to ""Be our hero. Be our silent guardian. Be our watchful protector. Be our Cyber Knight."[274]

[274] Raytheon, 'Bursaries For Superheroes - Raytheon Funds Bursaries for Student Cyber Defenders', 19 October 2017, https://perma.cc/CVX8-L9S4.

The ambiguity of military experience was replicated for those with connections to intelligence agencies. As I demonstrate in Chapters 7 and 8, many cybersecurity organisations are closely entangled with intelligence agencies. I sometimes encountered intelligence professionals at cybersecurity conferences who were identifiable because they refused to say where they worked, to give me a business card or talk about their views or background in cybersecurity. After several such encounters I asked others about these individuals, with the swift reply that they were from the national intelligence service. Some interviewees saw a background in intelligence as a valuable commodity in becoming a credible cybersecurity expert. As one interviewee put it, "if you're ex-NSA or GCHQ [the US and UK signals intelligence agencies], the natural assumption is that you're a good egg" (I-41).

However, in other cases intelligence backgrounds were seen as negative. When I asked another interviewee whether commercial experience was essential for cybersecurity expertise, he agreed, with the qualification that "the intelligence community pushes the other view, as they occupy senior positions in cybersecurity. They have a heightened awareness of what nation states can or are doing. People want to personalise who the bad guy is" (I-44). The intelligence community's perspective of cybersecurity as a 'personalised' and almost ideological adversarial competition was seen by this interviewee as an influential frame for cybersecurity overall, due to the 'senior' roles occupied by former intelligence officials. Another interviewee expanded on the problems of such senior intelligence officials in cybersecurity:

> People come over from the UK, or elsewhere, and tell you they have 10 years' experience, this government, that government, but when you drill them it's not the right kind. Cybersecurity here is flooded with people who worked in intelligence, but it is different! It's not the same as what you did in the '70s or '80s. This makes working on cyber issues very difficult, as to get funding you need to have approval, but someone who's consulting who claims a background but doesn't have it. They might have 20 years on their CV but it's not the right job (I-40).

This quotation weaves together several threads of cybersecurity expertise considered in this section. First, there is the CV-based element of expertise, including education and qualifications and the strategic self-promotion common in the cybersecurity expert community, of someone "who claims a background but doesn't have it". Second, there is the view that the speed and novelty of

technological change makes pre-internet experience irrelevant: cybersecurity is "not the same" as previous issues. Third, and finally, there is the ambiguous position of former government and intelligence professionals who 'flood' cybersecurity. The construction of a cybersecurity expert community through qualifications and experience, then, is not a simple matter of exams or certificates, but a multifaceted and complex product of age, experience, status, and education.

4.3.2 Nationality

The second aspect of cybersecurity expertise in Egypt and the Gulf states that contributes to the creation of an ambiguous professional discourse is interaction between different nationalities. Nationalities are not fixed categories based on passport information, but more complex constructions from visible ethnicity, accent, and other aspects of an expert's habitus. A common theme in interviews in the Gulf states was the large number of expatriate workers in cybersecurity, which reflects their long symbiosis with external labour, especially from South Asia. Some interviewees, both expatriates and local nationals, saw this diversity positively, with one saying that "the IT space is all expats, but I don't see a disadvantage when it comes to IT security based on nationality." (I-48). A Qatari interviewee argued the following:

> We will always be dependent on foreign labour, like the US, Europe, everywhere else. Nowhere is there 100% employment of nationals. We need to rely on a highly skilled workforce, we need to engage and recruit them from elsewhere. Everyone is doing it and we no less than the others. Diversity is good! (I-4).

However, this reliance on global labour patterns conflicts with national security restrictions across the Gulf states. As an Omani national put it: "Information security has to be Omani for the government, and there is a shortage" (I-5). In Bahrain, an interviewee attributed these restrictions to sectarian divisions, given Bahrain's large Shia population: "Whether you are Shia or Sunni makes a difference in recruitment, and whether you have connections as well" (I-31). Similarly, an interviewee in the Saudi Arabian government said that:

> In security we have more Saudis than foreigners... This is a government requirement, whether it is written down or not. When we are hiring in other positions, Saudis are not preferred, but here in security we hire Saudis wherever possible. Because it is the critical infrastructure of the country – cyber war, you know? (I-51).

This also fits in with wider Gulf government efforts to nationalise their workforce, with longstanding policies in all GCC states cited by many interviewees. Nationality was also perceived to assist technical communications: for example, one interviewee said that "[I]t is also a cultural thing: I am able to explain something in a way which makes sense to them, and a foreigner couldn't do that. It makes a big difference" (I-53).

The result, however, is a perceived power differential between expatriates and nationals, mirroring wider labour inequalities. A UK national described his experience as such: "In Middle East organisations the decision maker at the top will be a local national, and below them there is a series of consultants" (I-47). Crucially, this affects the nature of cybersecurity expertise itself, as "there is a lot of saving face by lots of people in key roles… they have no trust to their board because of their nationality" (I-42). An Indian national described how a 'friend' had altered their advice due to an extremely unequal power relationship:

> A friend from South Asia gave a final audit, but he was told by a UAE senior to 'get out of the room now'. You need to present it as 'risk is a risk, but it is not a fault'. Managers take criticism less easily from expats than from Omanis (I-28).

Egypt and the GCC states have a complicated relationship within these broader power dynamics. The longest running cybersecurity conference in Egypt, Cairo Security Camp, is the nearest to a 'hacker' conference of the seven cybersecurity conferences I attended, both in terms of the content of the presentations and their anti-establishment tone, and also in the status symbols displayed by attendees (webcam covers, laptop stickers, dress code, and so on). However, many Egyptian nationals move to the Gulf to work in cybersecurity, again reflecting wider labour flows. Attendees at this conference thus translate their technical skills into a commodity on the international labour market:

> A lot of Egyptians are well trained, but they leave Egypt. Especially at Cairo Security Camp – the conference you saw was pretty much all the people who are interested in it. After they present they go to the big companies, to Europe or the Gulf. (I-12).

This has both advantages and disadvantages. On one hand, Egyptian expatriates recognised that their cultural identity could be an advantage: "As an Arab I have a strange role, neither local nor foreign. It's better to be an Arab than an expat, but even better to be a national." (I-21). There are thus opportunities for strategic advantage even within the perceived hierarchy of nationalities. On the other hand, the emigration of cybersecurity professionals from Egypt to the Gulf creates problems for those who remain in Egypt. As one interviewee noted:

> We could have a large security community, but they are being attracted by better offers from the Gulf and Europe. The problem is to find and maintain these people, we develop them but others offer better. I would like to change this, as you have to maintain your own local force. We don't want to reinvent the wheel, but Qatar or Kuwait are an unfair comparison (I-35).

This mix of nationalities means that the role of the Arabic language in the professional discourse is important. Although I consider the implications of translating 'cybersecurity' into Arabic in Chapter 7, here I highlight the view of many interviewees that Arabic is unsuited to technical discussion. For example, two conference speakers I watched began their presentation in Arabic and then switched to English, apologising with the excuse that it is easier to talk about cybersecurity in English than in Arabic (ARCC2016). More bluntly, one interviewee said that "cybersecurity can't be taught in Arabic, it is a foreign concept" (I-37). Others agreed:

> Official comms and government all use Arabic, but it's not easy as you can't find synonyms. You can't tell the exact meaning of *sibrani* [the loan word for 'cyber']… *sibrani* – what does it mean? At least people relate *muʿalumat* [information] to a word they understand (I-17).

> You can't talk technical in Arabic. Things like cyberspace, APT [Advanced Persistent Threat], TI [Threat Intelligence], are all in English. We were trying to think of the word for 'login' in Arabic – someone used *iʿtiraf* [meaning acknowledgement or admission in the sense of guilt, rather than permission]. It's not right! (I-52).

Consequently, although the legal and policy sectors translate key terms into Arabic, it is rarely used by the expert community. Some interviewees located this ineffectiveness within longer-term disparities in technological development. As one of the interviewees above argued, "we will never enforce Arabic until we produce the technology… As long as we are consuming, we will use the language of the producers" (I-17). However, other interviewees emphasised that Arabic was

nonetheless useful in certain situations. One said that "this is another factor which helps me sell. It's all about communicating effectively, but [customers] prefer the Arabic language" (I-38).

In sum, the national identities of cybersecurity experts interact in multiple ways to define the contours of the cybersecurity professional community in the region. This is a highly skilled, well educated, international community, including consultants and technical experts who travel regularly around the world. Consequently, these experts are used to working in a mixed-nationality environment and using the international business and technology language of English. However, within this environment there are clear hierarchies and distinctions, between expatriates and local nationals, Egyptian and Gulf Arabs, and between different expatriate nationalities. In negotiating these hierarchies, cybersecurity experts build multiple layers of ambiguity into the professional discourse: through carefully judged messages of risk, in selling and training cybersecurity for different audiences, and even in their choice between Arabic and English in different contexts.

4.3.3 Gender

The final section of this chapter briefly considers the role of gender in cybersecurity expertise in Egypt and the Gulf states. This is a large topic and deserves more sustained examination than permitted by the scope of this thesis, as well as systematic connection to existing theories of gender in IR and Middle East studies.[275] This brief overview provides only an initial reading, based on a research design that seeks to avoid perpetuating silence over gender issues in academic treatments of cybersecurity. To this end, I asked about gender dynamics in cybersecurity in interviews only where it felt appropriate to do so given my positionality.

Firstly, at a general level, cybersecurity expertise is gendered in several ways. Differentiation by sex can be illustrated in a simple statistic: of the 96 most frequent speakers at the 165 cybersecurity conferences I analysed, only 4 of these speakers were female. Interviewees all

[275] Madawi Al-Rasheed, *A Most Masculine State: Gender, Politics and Religion in Saudi Arabia* (Cambridge: Cambridge University Press, 2013); Lila Abu-Lughod, ed., *Remaking Women: Feminism and Modernity in the Middle East* (Princeton, N.J: Princeton University Press, 1998); Deniz Kandiyoti, ed., *Gendering the Middle East: Alternative Perspectives* (London: I.B.Tauris, 1995).

noted the gender imbalance in cybersecurity professionals, with one claiming that "cybersecurity is dominated by men" (I-55). This is on one level unsurprising. It is similar to many other science, technology, engineering and mathematics (STEM) fields worldwide, and also follows gender inequality in many areas of the workforce in Egypt and the Gulf states. However, a few interviewees claimed that in engineering schools in the smaller Gulf states around half of cybersecurity graduates who are also citizens of those countries were female.

Gender analysis involves more than a simple numerical comparison between sexes. It was clear in my interviews that concepts of masculinity and femininity permeated interviewees' ideas of cybersecurity expertise. Masculinity is generally understood as a collection of qualities contingently associated with the male sex, although some feminist theorists argue that its conceptual cohesion is provided instead by dominance or positive valence in opposition to a set of negatively valued or oppressed 'feminine' qualities.[276] Masculinity and femininity are not innate but are performed in specific social and cultural contexts. In the Middle East questions of gender are also intimately associated with colonial notions of modernisation and progress on the one hand and religious understandings of authenticity and appropriate conduct on the other. Each of these complex streams of thought shapes the understanding of gender in cybersecurity, and interviewees often recognised this complexity. For example, an Egyptian national (based in Egypt) said:

> I am not happy about gender balance statements, unless we have put up a barrier in the way we teach or train. There is a concern about working 24/7, and women should get different shifts to men. I think we should provide a working environment which is suitable for everyone, but equality is a different question. If I have to have someone come out at midnight [for an emergency call], then coming from the Middle East there is no easy way to discuss this. However, we provide maternity leave, which the US doesn't!" (I-24).

Other interviewees associated cybersecurity expertise itself with a militarised understanding of masculinity including characteristics such as toughness and an attraction to technology. As one interviewee put it, "you don't hear about many female hackers. It's still a tough thing, requires not normal skills – it's a keyboard, not a gun or hammer, but still" (I-35). These interviewees contrasted

[276] Jane L. Parpart and Marysia Zalewski, eds., *Rethinking the Man Question: Sex, Gender and Violence in International Relations* (London: New York: Zed Books, 2008)

an implicitly valorised militarised masculinity to a soft, weak construction of femininity to explain the gender imbalance above: “There is just no interest in tech from women! It’s all boys playing computer games at age 15. It’s the same as women in combat – of course they run faster than me, but they have a motherly instinct” (I-27).

Other interviewees constructed a different understanding of femininity which was portrayed as advantageous for cybersecurity expertise. One interviewee said that “I read something about women being better at emotional intelligence, so they would be better at strategic decisions” (I-55), while another commented that “if I decided, then I would make 70% of the cyber security people women, because they are better at following procedures” (I-51). This particular cybersecurity femininity does not directly contradict the version above, but emphasises different qualities – rule-following, emotional intelligence – to incorporate femininity into the identity of a cybersecurity expert. However, this remains within a masculine/feminine hierarchy where the masculine cybersecurity expert is in a position of decision and rule-setting, while the feminine expert follows those rules.

It is important to note that all the quotations above are from male interviewees. It was notable that the six women I interviewed did not want to comment on gender, or simply said that the gender balance was improving, citing university male/female ratios. This reluctance to comment may be due to their experiences in a highly unequal environment, or it may be due to the atmosphere of interview performance with a male interviewer. Either way, this constraint means that further work is needed to understand female voices in cybersecurity. It is sufficient for the argument of this thesis that the gender dimensions of cybersecurity are seen by its participants as ambiguous, and form part of a wider uncertainty about the ‘correct’ way to perform cybersecurity expertise.

***

This section has demonstrated the complexity of cybersecurity expert identities, which are gendered, informed by nationality and language, and have an ambivalent relationship with education, experience and professional qualifications. This complexity is a key source of the ambiguous

professional discourse that enables the moral manoeuvres examined in Part 2. This ambiguous discourse is thus not only inherited through the broader genealogy of cybersecurity but amplified by the contours of the professional community considered here. I conclude this chapter with a voice from this community itself. As one interviewee admonished me after one too many questions about expertise:

> "Don't just say 'expertise', some people have more technical expertise and management expertise. You need a team – look for advocates, no one person can work alone. There is not one profile, but the team needs to be integrated, it needs to have champions in all sectors. You can use terms and language that are closer to different sectors. ICS [industrial control systems] specialists and computer system analysts are important but they require different levels of expertise…They need to know the details, for example of the electric grid. An electricity expert would know you cannot disrupt the flow, and so it is about compromise, or a pragmatic understanding" (I-24).

For this interviewee, cybersecurity expertise is an amalgam of many technical disciplines, as well as the social and political characteristics sketched above. The role of these disciplines in shaping the understanding of key cybersecurity incidents in the region is the subject of the next chapter.

Chapter 5. Events

At the start of a conference presentation I attended, a cybersecurity expert played a realistic-looking video of a power plant. The scene was calm, and workers were going about their ordinary business: driving trucks, carrying clipboards, walking along in intense discussion, and just waiting around. Suddenly, an explosion ripped through the plant, as a building to the right of frame disintegrated. Trucks swerved and were blown onto their side, people scattered in all directions, and a lick of flame shot across the screen. The presenter stopped the video, with the warning that although this was not a cybersecurity incident, *it could have been* (RSAAD2016).

In this chapter, I trace the emergence of a professional cybersecurity discourse in Egypt and the Gulf states through the lens of cybersecurity incidents ('events' for short) in these seven states. This follows on from the investigation of cybersecurity expertise in the previous chapter, as information about these events is created, analysed and disseminated by cybersecurity experts, both within the region and outside it. Moreover, cybersecurity expertise, fundamentally understood as the judgement of cybersecurity risks, is empirically based on a limited set of incidents that represent risks realised or nearly realised. Although cybersecurity professionals collect large amounts of data to assess cybersecurity risks, they nonetheless resort to illustrations based on these key events to demonstrate the severity of the cybersecurity threat to both expert and non-expert audiences. This chapter is based primarily on a discourse analysis of technical incident reports of key cybersecurity incidents and surrounding media coverage, with interviews also used in the second section.

The chapter has three sections. The first section outlines early cybersecurity incidents in the region. The second section examines the most well-known and influential cybersecurity incident: the 2012 Shamoon malware in Saudi Aramco and RasGas, sketched briefly in the introduction to the thesis, and its 2016 reoccurrence. The third section explores other cybersecurity incidents in two categories of cyber espionage and hacktivism. This section then synthesises all the events in this chapter to argue that together they constitute a generic 'organisational' cluster of values of cybersecurity that incorporates substantial ambiguity towards its referent. This ambiguity is

engendered by both technological characteristics and professional incentives and enables the four moral manoeuvres detailed in Part 2.

5.1 Origins

Analysts have noted multiple dimensions to cybersecurity discourses in the US and Europe for at least two decades. In 2002, Deibert identified four interlocking images of what he called 'internet security': national security, state security, private security and network security.[277] The year before, Bendrath observed that several cybersecurity risk perceptions existed simultaneously in the US, including threats from military rivals, terrorism, and economic loss. As he noted, terrorism was an especially salient term:

> The U.S. National Academy of Sciences as early as 1990 begun a report on computer security with these words: "We are at risk. Increasingly, America depends on computers. [...] Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." This quote is typical for a whole series of warnings issued by the intelligence community, the FBI and other government agencies in the last ten years.[278]

Bendrath put these different perceptions in the context of 'failed' securitisations, which attempted to raise awareness of cybersecurity at a national level. Seven years later, in her analysis of the US cybersecurity debate, Dunn Cavelty demonstrated that this securitisation was partly successful after 9/11 and the consequent establishment of the US Department of Homeland Security, as "the focus of attention shifted from hackers depicted as terrorists towards terrorist hackers, and specifically Muslim ones."[279] This was combined with the rise in the concept of 'critical infrastructure' as a vulnerable object that could be threatened by cyber or physical means.[280]

In the Middle East, cybersecurity issues first emerged in relation to longstanding conflicts. In 2001, Lawson noticed how reciprocal website defacements – the unauthorised writing of political text or uploading political images on websites - between hackers in Israel and Palestine quickly

[277] Deibert, 'Circuits of Power: Security in the Internet Environment'.
[278] Bendrath, 'The Cyberwar Debate', p.81.
[279] Dunn Cavelty, *Cyber-Security and Threat Politics*, p.118.
[280] Claudia Aradau, 'Security That Matters: Critical Infrastructure and Objects of Protection', *Security Dialogue* 41, no. 5 (1 October 2010): 491–514.

became framed as a 'cyberwar' or 'cyber-intifada'. In this article, Lawson cited a 'Middle East security consultant' as claiming, in relation to the vulnerability of Saudi Arabian networks to this supposed cyberwar, that "the Israelis know where and how to target their attacks because many Middle East networks rely on the firewall software called Checkpoint, which is an Israeli-produced product that Israelis no doubt know how to defeat".[281] Although the threat of Israeli cyber espionage identified by the Saudi consultant would be realised a decade later, this highlights how even the first cybersecurity companies were seen within a national security lens, especially in the highly polarised political economy of the Middle East.

The post-9/11 US foreign policy priority of Islamist terrorism not only assisted the US securitisation of cyberspace, as argued by Dunn Cavelty, but also encouraged the professional cybersecurity community to focus its attention on Egypt and the Gulf states. For example, US cybersecurity company Symantec included a cyber-terrorism watchlist in their regular cybersecurity threat reports in 2002 and 2003. This watchlist encompassed Egypt, Saudi Arabia, Kuwait and the UAE among others, reflecting increased US tensions with the Gulf due to the Saudi Arabian origin of most of the 9/11 hijackers. Interestingly, in their threat reports Symantec emphasised that even though they "do not claim to have specific expertise in terrorism" they still felt able to monitor "some of the more likely sources".[282] Overall, these two trends - US concerns around cyberterrorism and the 'cyber-intifada' – were the first links between cybersecurity and national security values in the Middle East.

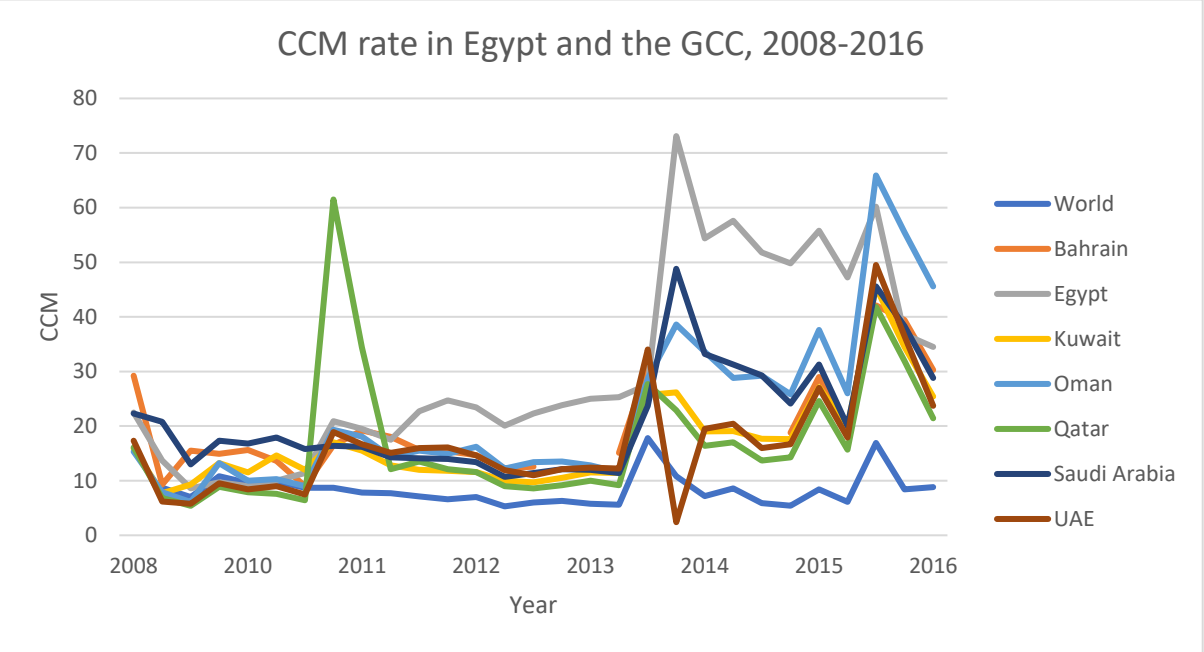
In contrast, the next phase in the emergence of cybersecurity in Egypt and the Gulf states characterised cybersecurity as primarily an economic issue. Trojans, worms and malicious software, most of it operated for financial gain, were tracked worldwide by cybersecurity companies from 2002. A survey of annual threat reports published by nine companies provides an overall picture of the region.[283] Given the flawed measurement processes at the time – e.g. tracking the origin of

[281] Sean Lawson, 'Cyber-Intifada Resource Guide: A Resource for Tracking the Intifada in Cyberspace' (The Arab Information Project, Georgetown University, 2001), p.9.
[282] Riptech [now Symantec] Internet Security Threat Report, Volume II, July 2002, p.15.
[283] The companies are as follows, with first year of reporting in brackets: Cisco (2010), Kaspersky (2006), Symantec (2002), Mandiant (later FireEye) (2010), McAfee (later Intel Security) (2009), Microsoft (2008), PWC (2016), RSA (2015), and Verizon (2008).

malware through the country location of the IP address it connects to – their conclusions should be treated with caution. Symantec reports claim that Egypt was frequently one of the top sources for malware per internet capita (i.e. individuals with access to the internet) between 2002 and 2011, and in 2010 it was also one of the top virus-contributing countries worldwide. McAfee and Cisco reports identify Saudi Arabia as a key source of spam in 2012 and 2013 respectively, while Egypt is consistently in McAfee's list of countries with many servers hosting malicious content from 2012. Verizon reports identify early data breaches in all seven states, beginning with Egypt (2010), UAE (2011), and Kuwait (2012).

From 2008, Microsoft provides a measurement of 'computers cleaned per mille' (CCM), which is the number of infections detected per thousand computers running Microsoft security services, broken down by state. The CCM can be taken as an indication of the prevalence of malware in that state, as displayed in Figure 2. According to this data, until 2011 malware levels in Egypt and the GCC were slightly higher than the global average, with a split between Saudi Arabia, Kuwait, and Bahrain as consistently higher and Oman, UAE, and Qatar as equal or lower. Saudi Arabia generally had a higher malware level than the rest of the GCC from the earliest report in 2002, although Egypt had the highest level of the seven states between 2011 and 2015. After 2011, Egypt and the Gulf states were all significantly above the global average, with a clear increase from mid-2013. The reason for the spike for Qatar in 2011 is unclear but may be due to its small and highly connected population; one large malware infection would drastically alter the CCM rate.

Figure 2: CCM rate in Egypt and GCC, 2008-2016



Overall, these reports created a perception of the region as a source of cybersecurity threats to businesses, suggesting an economic rather than national security referent. However, they also had a more fundamental effect on the cybersecurity professional discourse in Egypt and the Gulf states, as they were generated by US companies moving into global markets, and so the statistics above were designed to generate business for these specialised companies in non-Western regions. As Dunn Cavelty and Balzacq write:

> Cyber-security reports… visualise malware based on the collection of data about infected machines, which is then aggregated in terms of infection rates per country. The practice of aggregating malware infection this way performs a version of the social in which space is exclusive: there are neat divisions with no overlap, based on a comfortable geography of well-known political entities. This allows identifying the 'good' from the 'bad' as well as the areas that are most in need for intervention. Whereas every locale in which there are computers/computer networks is a (potential) space for cyber-security, the focus on infection rates per country easily translates into regions of in-security.[284]

In Dunn Cavelty and Balzacq's terms, these cybersecurity reports construct Egypt and the Gulf states as a 'region of insecurity'. Although accurate, I go beyond this claim to argue that this

[284] Balzacq and Cavelty, 'A Theory of Actor-Network for Cyber-Security', p.13.

insecurity is inherently *ambiguous.* To dissect the origins of this ambiguity, I focus on one early cybersecurity event in Egypt.

In 2009, an FBI operation conducted jointly with the Egyptian authorities arrested around 100 people, 43 of whom were in Egypt. These arrests were linked to an online scam named 'Phish Phry', in which phishing emails were sent to Bank of America customers to obtain their login details, with $1.5 million taken from victim accounts.[285] 'Phishing' is a cybersecurity term for the gathering of credentials such as usernames and passwords through illegitimate versions of websites. Importantly, a statement by Robert Mueller, then-FBI director, after the arrests brought together concepts of both economic and national security. In his statement, Mueller warned that:

> What may start as a criminal investigation may lead to a national security threat. … At the start of a cyber investigation, we do not know whether we are dealing with a spy, a company insider, or an organised criminal group.[286]

This ambiguity between different referents is based on professional cybersecurity practices developed in tandem with the technological characteristics of the issue area itself. In most cybersecurity investigations the attacker or adversary is given a codename based on mainly technical identifiers, as their identity can be hard to determine from the perspective of the investigator without recourse to national-level intelligence capabilities. In such cases, plausible identities can be inferred from the assumed motive of the adversary, itself based on details of the target. Mueller's statement above can therefore be read as simply explaining this aspect of 'cyber investigations'.

However, Mueller also used this ambiguity to expand the relevant security frames around Phish Phry by stating that "something that looks like an ordinary phishing scam may be an attempt by a terrorist group to raise funding for an operation".[287] Here, despite no indication of any link to terrorist groups, Phish Phry was placed in a national security frame. The creation of a region of insecurity identified by Dunn Cavelty and Balzacq thus interweaves economic and political concepts together into a single *ambiguous* cybersecurity discourse.

---

[285] Kim Zetter, 'Gang of 100 Phishers Charged in U.S., Egypt', Wired, 7 October 2009, https://perma.cc/M9R8-J49Y.
[286] FBI, 'Operation "Phish Phry"', FBI, 7 October 2009, https://perma.cc/LFJ5-KSDH.
[287] FBI.

It is instructive to compare the US characterisation of Phish Phry with the Egyptian version. Arabic sources indicate that there was a domestic professional community interested in these issues at least from 2009, when the arrests took place. Likely Egyptian users of a Saudi-based IT forum posted technical details of the Phish Phry scam the day after the arrests were reported in the US media. One forum post said that "their wealth appeared suddenly, they were talked about in the area and everyone knew their story but they were not arrested until after years of hacking" (*zuhira ʿalaihum al-thuraʾ fajaʾatan wa tamm tadawul muʿalumat ʿanhum fi al-balda wa asbaha al-jamiʿa yaʿarifu qisatahum wa lakin lam yatimm al-qabd ʿalaihum ila baʿad sanawat min al-qarsana*).[288] However, it also said that "many of the accused were forced to confess and sign written reports after they faced beatings and torture and repeated insults" (*ʿadadan min al-muttahamin tamm ijbarahum ʿala al-ʾitiraf wa al-tawqiʿi ʿala ʾiqrarat maktuba baʿad ʾan taʿarradu lil-darb wa al-taʿdhib wa lil-ʾihanat al-mutakarrara*).[289] While these details are unconfirmed, if true they highlight the early involvement of the Egyptian security services (*ʾamn al-dawla*) in cybersecurity investigations and the incorporation of cybersecurity into the violent national security practices of the Egyptian state, and the expansive definition of national security detailed in Chapter 3.

In contrast, articles on Phish Phry in the mainstream Egyptian media did not mention these details, with Phish Phry labelled as 'the issue of electronic piracy/hacking' (*al-qadiat al-qarsanat al-ʾiliktruniyya*) in national newspapers Al-Masry Al-Youm and Al-Watan. The description of Phish Phry as *qarsana* initially had more of a connotation of theft than illicit entry, although *qarsana* is now used for both piracy and hacking generally, and the absence of a clear translation of the prefix 'cyber' into Arabic meant that 'electronic' was the accepted substitution. Furthermore, according to these media reports, witnesses included the information network department in the interior ministry, the computer crimes department in the police, and the national telecommunications agency.[290] This

[288] Mzdr, 'Tamm Al-Qabd ʿala Qarsanat Al-Bunuk Al-Amrikiyya Fi Misr [Arrests in Egypt over Piracy against the American Banks]', Swalif Soft, 13 October 2009, https://perma.cc/MD8L-UZQJ.
[289] Mzdr.
[290] Ghada ʿAbd Al-Hafiz, 'Janayat Al-Mansura Tuʾajjilu Mahkamat Al-Muttahamin Fi Qadiyyat "Al-Qarsanat Al-ʾiliktruniyya" ʾila 2 Mayo [Mansoura Court Postpones Sentencing in the Case of "Electronic Piracy" to 2 May]', Al-Masry Al-Youm, 6 March 2010, https://perma.cc/AV3P-6CAZ.

combination of government departments is an interesting anticipation of the struggles between different state organisations over the ownership of cybersecurity expertise explored in Part 2.

While the US-based members of the Phish Phry gang were given prison sentences,[291] Egypt's turbulent political situation meant that the Phish Phry operation (with arrests taking place in October 2009) was largely overshadowed by the January 2011 revolution. Interviews in Al-Masry Al-Youm with families of the Phish Phry defendants emphasised the revolution as a turning point in this case, claiming that "the citizen raised his head after the revolution… they [the defendants] are part of the free future of Egypt" (*rafaʿa almuwatin raʾasahu baʿad al-thawra… hum juzaʾ min mustaqbal misr al-hurra*).[292] These interviews also cited as an indication of their honesty that "there was a chance to escape during the revolution but they did not try to escape" (*kana ʾamamhum fursa lil-hurub ʾathnaʾ ʾahdath al-thawra ʾila ʾanhum lam yuhawalu al-hurub*).[293] Consequently, after six years, the Egyptian defendants were acquitted in 2015, reportedly with no analysis of the large amount of data provided by the FBI to their Egyptian counterparts.[294]

In sum, the Phish Phry incident looks very different from the US and Egyptian lenses. For the US, although Phish Phry was a criminal gang, it could have been a terrorist group fundraising large amounts of money due to the inclusion of Egypt in an ambiguous 'region of insecurity'. For some Egyptian observers, Phish Phry was merely one of many ways for educated young men to use their technological skills in a way accepted by their local community, although this event also highlighted the assimilation of cybersecurity into the routinised violence of the Egyptian security forces and the expansive definition of national security prevalent especially after the January 2011 revolution. Finally, it is worth noting that the Phish Phry scam also anticipated a similar incident in the Gulf three years later, when there were two separate compromises of prepaid credit card information for

[291] Bill Singer, 'Feds Catch Their Illegal Limit In Operation Phish Phry', Forbes, 15 May 2012, https://perma.cc/ZDL7-Z59U.
[292] Ghada ʿAbd Al-Hafiz, 'Tuʾajjal Mahkama 43 Shaʿaban Fi Qadiyyat Al-Qarsanat Al-ʾiliktruniyya ʾila ʾabril [Trial of 43 Youths in Electronic Piracy Case Postponed until April]', Al-Monitor, 18 February 2011, https://perma.cc/8XNV-X9NN.
[293] ʿAbd Al-Hafiz.
[294] ʾAhmad Shalbi, 'Janayat Al-Mansura Tubarriʾu 41 Mutaman Min Sariqa Milliyiyin Al-Dularat Bi 3 Bunuk ʾamrikiyya [Mansoura Court Exonerates 41 People Accused of the Theft of Millions of Dollars from 3 American Banks]', Al-Masry Al-Youm, 9 September 2015, https://perma.cc/FF7U-3C3B.

customers of BankMuscat in Oman and RAKBank in the UAE in December 2012 and February 2013.[295] This information was also provided to a transnational criminal network who withdrew $45 million in cash from ATMs across the world using those card details.[296]

5.2 Two Shamoons

I now focus on one event in particular: the Shamoon incident with which I began the thesis. I draw on the same sources as the section above - technical reports and surrounding media – as well as interviews with cybersecurity professionals in the region. I use this closer analysis to explore several themes noted above: the ambiguity between different conceptions of cybersecurity; the relationship between international and local framings of cybersecurity incidents; and the emergence of discursive patterns of codenames, technical data, and concepts of destruction. As well as the ambiguity that is a core plank of the thesis argument, the latter two themes form the basis for the moral manoeuvre of alignment detailed in Chapter 6. The label Shamoon has been used to refer to two separate incidents in 2012 and 2016; I refer to them as Shamoon 1 and Shamoon 2.

5.2.1 Shamoon 1

In August 2012, malware spread through the business networks of the Saudi national oil company, Saudi Aramco, and wiped data from around 30,000 computers. A few weeks later the Qatari gas company RasGas was affected by the same malware. According to Saudi officials, the aim of the operation was to "stop the flow of Saudi oil".[297] Shamoon 1 was described as a "wake-up call" by a senior US cybersecurity official, claiming that "a similar attack on our critical infrastructure networks could have grave effects on financial markets, communication networks, and

[295] Brian Krebs, 'Crooks Net Millions in Coordinated ATM Heists', *Krebs on Security* (blog), February 2013, https://perma.cc/9MSZ-QJ8F.
[296] Marc Santora, 'In Hours, Thieves Took $45 Million in A.T.M. Scheme', *The New York Times*, 9 May 2013, https://perma.cc/3A8A-5RG6.
[297] Mahdi, 'Saudi Arabia Says Aramco Cyberattack Came From Foreign States'.

health and safety services".[298] The US Defence Secretary cited Shamoon 1 in a speech warning of a "cyber Pearl Harbor".[299] It has consequently become a standard reference for 'destructive cyber-attacks' in IR, and I will return to this phrase below.[300]

The technical details of Shamoon 1 were determined early on by the analysis undertaken by three cybersecurity companies - Symantec, Kaspersky, and Seculert - all published on 16 August 2012.[301] These analyses revealed that the malware used a component named 'Wiper' to overwrite data on the hard drive of the infected computer in a very simple way: it sequentially worked through all the files on the computer, replacing them with the image of a burning US flag. Finally, it overwrote the computer's master boot record, causing the computer to lose all functionality. In general, one can overwrite data for many legitimate purposes, and the specific overwriting application used in Wiper also has many benign applications. However, this particular 'Wiper' component had a similar wiping process to a module in Flame, a US espionage operation detected in Iran earlier in 2012. The reports about Shamoon 1 describe Shamoon 1 either as reengineered, emphasising the same technical properties as Flame, or as a copycat, suggesting it was a technically distinct imitation.[302]

The name of the malware is itself a socio-technical construction. The cybersecurity companies noticed that its file location was "C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb". They took the name 'Shamoon' from this filename and used it to refer to the malware as a whole. Kaspersky speculated on the origin of the name: "it could be a reference to the Shamoon College of Engineering… [in Israel] Or, it could simply be the name of one of the malware authors. Shamoon is the equivalent of Simon in Arabic."[303] While these assessments were judged incorrect by the wider

[298] Infosecurity, 'Saudi Aramco Cyber Attacks a "Wake-up Call", Says Former NSA Boss'.
[299] Bumiller and Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.'
[300] Bronk and Tikk-Ringas, 'The Cyber Attack on Saudi Aramco'.
[301] Aviv Raff, 'Shamoon, a Two-Stage Targeted Attack', *Seculert Blog on Advanced Persistent Threats and Malware* (blog), 16 August 2012, https://perma.cc/2PNQ-5XTE; Kaspersky Lab, 'Shamoon the Wiper - Copycats at Work', Securelist - GREAT, 16 August 2012, https://perma.cc/48ZN-JT7Z; Symantec Security Response, 'The Shamoon Attacks', 16 August 2012, https://perma.cc/BS32-A7BW.
[302] Kaspersky Lab, 'Shamoon the Wiper - Copycats at Work'.
[303] Kaspersky Lab.

community, they were nonetheless an attractive hook on which to advertise the company's services. The name therefore gained salience due to both malware characteristics and professional positioning.

A group called "The Cutting Sword of Justice" claimed responsibility for Shamoon 1 through a message left on Pastebin, a site often used by hacktivists and others to claim website defacements:

> We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.[304] [dots not inserted]

This message appears to provide a 'hacktivist' motivation for the incident. However, Shamoon was soon cited by US media as Iranian retaliation for previous cyber operations against Iran by the US and Israel.[305] The public consensus, likely encouraged by classified intelligence from government agencies in the UK and US, was that Iran was ultimately responsible for the incident.

My interviews with cybersecurity professionals in the region underline the effect that Shamoon 1 had on cybersecurity in the region. One interviewee echoed the language of the US officials quoted in the Introduction, saying that "the breach of Aramco was a wake-up call in general, in the eyes of everybody, we realised that the Middle East is not isolated" (I-17). A Qatari official expressed this shift in terms of the tangibility of cyber threats, saying that "after RasGas, you were able to see it, we felt them" (I-4). Another interviewee also used the metaphor of awakening:

> Shamoon was the real wake up call. In meetings shortly afterwards, people realised what it could do. It was all about the GDP of the country, and the country relies on O&G [oil and gas], that's why it had a big effect. Before then, people were just doing cyber because they felt they should do cyber. (I-13).

Although Shamoon 1 only targeted data on business networks, cybersecurity experts interpreted it as also demonstrating risks for critical infrastructure. As one interviewee put it, "Aramco shocked everyone, even the man on the street. We were worried our pipelines might stop

[304] Cutting Sword of Justice, 'Untitled', Pastebin.com, 15 August 2012, https://perma.cc/4KZZ-GGRF.
[305] Perlroth, 'Cyberattack on Saudi Oil Firm Disquiets U.S.'

pumping oil" (I-49). Another interviewee stressed this transfer of risk from business to operational networks:

> In the Aramco attack, they were not targeting ICS [industrial control systems], they were targeting the business. But it woke them up to improve ICS because some ICS were affected because they were connected, even without realising it… Aramco was lucky to have this attack, as it could have done major destruction. Other companies will tell you it was an ICS attack, but ICS effect was not the target (I-3).

Other interviewees highlighted the commercial benefits of Shamoon 1 for the cybersecurity industry in the region. An interviewee based in the UAE said that "Aramco was the main incident that happened, and it really helped our momentum" (I-26). A Bahraini interviewee compared the effect favourably with Stuxnet, a US-Israeli cyberattack on an Iranian uranium enrichment facility, explaining: "Aramco had a huge impact here, the Iranian attack was not as important because it was not a commercial establishment" (I-31). The increased salience of cybersecurity led to a clear response from their customers. As one interviewee said, "before Shamoon, people were fussy on the details, and would agree that cyber is important but not willing to spend money on it" (I-13). After Shamoon 1, financial commitment was seen as matching organisational changes:

> Before Aramco cybersecurity was part of the IT department, under an IT manager. In O&G [oil and gas] the CTO [Chief Technology Officer], the technical operations people, thought they were the priority, and IT was just back office like HR [human resources] or something. The operations people brought in the money, and did the important stuff… After Aramco everything changed: for a couple of years they spent a lot, and bought everything, all the latest technology (I-12).

I now turn to the relationship between international and regional perceptions of Shamoon. Local coverage of the incident was almost non-existent in the first weeks after the event, which is in keeping with the quiescent and government-controlled nature of mainstream media outlets in Saudi Arabia. The stories that did run were either based on Western media or in outlets located in other countries. For example, an Arabic language technology website reported almost immediately on the incident, on 15 August.[306] It described Shamoon as penetration or hacking (*ikhtiraq*), theft (*sariqa*), and loss of data (*fiqdan al-bayanat*), but not as a destructive attack. Initially, this story stated that

[306] Saʿud Al-Hawawi, 'Musadir Khasa: Shabakat Sharikat ʾaramku Tataʿarrad Liʾikhtiraq Wa Almutasabbib Ahad Al-Muwazzifin [Private Sources: Aramco Company Networks Face a Hack and the Cause Is One of Their Employees]', ʿAlam Al-Tiqniyya, 15 August 2012, https://perma.cc/FHW6-JPUW.

Iran was involved, but a correction was immediately issued saying that "It is confirmed that Iran has no connection to this hack" (*tamm al-taʾakkud min muʿaluma biʾan ʾiran laisa liha ʿalaqa fi al-ikhtiraq*).[307] Another technology website posted the details of the incident online two weeks later, on 29 August, based on Symantec's first reports.[308] This post called the malware Shamoon, as did Symantec, and noted that it was based on a module from Flame, the US espionage malware against Iran discovered in 2010. Again, this post did not mention destruction, but it did call the incident an 'attack' (*hujum*).

In contrast, on 29 August 2012, Al-Jazeera published an Arabic-language article speculating on the actor behind the attack. In line with Al-Jazeera's political leanings, it stated that experts viewed Iran's involvement as unlikely and blamed a competitor in the oil industry. However, this article also cited a claim originally in the New York Times that the hack was political not economic (*siasi laisa tijari*) and mentioned that "probably there was an employee inside Aramco assisting the attack" (*ihtimalat ʾan yakun muwazzaf min dakhil ʾaramku sahal al-hujum*).[309] This article was the first to describe the incident as destructive, using the phrase *takhribi* (later coverage in the Al-Watan newspaper would also use the synonym *tadmiri*). The claim that an Aramco employee was involved (known as an 'insider') stemmed from a Reuters article on 7 September which stated that someone involved in the attack had inside knowledge and privileges.[310] Although later reports retracted this claim,[311] it was used by Al-Jazeera in the article above to politicise the incident further, and I will return to the significant concept of an insider in Chapter 9.

After a few months, when the international evidence of a significant cybersecurity incident was impossible to ignore, the Saudi media began to comment on Shamoon 1. The head of the investigative committee gave a press conference in December 2012, claiming that the aim was to

---

[307] Al-Hawawi.
[308] ʾAnas Al-Maʿrawi, 'Aramku Taʿtarifu Bitaʿarrud ʾanzimatiha Liʾikhtiraq Kabir [Aramco Admits Its Networks Faced a Large Hack]', *Aitnews*, 28 August 2012, https://perma.cc/ZC63-Z76W.
[309] Staff Report, 'Man Waraʾ Al-Hujum Alʾiliktruni ʿala ʾaramku? [Who Is behind the Electronic Attack on Aramco?]', Al-Jazeera, 29 August 2012, https://perma.cc/JT9H-HHKE.
[310] Jim Finkle, 'Exclusive: Insiders Suspected in Saudi Cyber Attack', *Reuters*, 7 September 2012, https://perma.cc/C5M6-WPWL.
[311] Staff Report, 'Shukuk Bishaʾan Muwazzafin Saʿadan ʿala Ikhtiraq Hawasib Aramku [Doubts over Employees' Help in Hacking Aramco Computers]', Al-ʿArab, 9 September 2012, https://perma.cc/Y8UR-WTRM.

damage Saudi Arabia's national economy.[312] His description of the attack used the by-then established phrases *hujum ʾiliktruni*, *qarsana* and *ikhtiraq*, and he countered the insider narrative by promising that no employee was involved or would be sanctioned because of the incident. He also stated that the attackers had tried to enter the Aramco networks for over a month.[313] A spokesman for the Saudi Ministry of Interior quoted by Al-Quds Al-Arabi (published in London) went further, and said that "Aramco was exposed to more than a process of piracy - it was electronic terrorism" (*taʿarradat lihu ʾaramku akbar min ʿamalia qarsana fahuwa ʾirhab ʾiliktruni*).[314] Later opinion pieces in Saudi-owned Al-Sharq Al-Awsat also labelled it as an act of terrorism after public association with Iranian actors.[315]

This analysis suggests that the trajectory of Shamoon 1 in the Arabic media had a complex relationship with its international English language coverage. On one hand, Arabic media relied on technical details from US cybersecurity companies and statements of attribution by US newspapers to publish opinion pieces in the more independent or anti-Saudi media outlets. On the other hand, the domestic Saudi media and Saudi-owned outlets were uncertain of the correct framing for this incident for a much longer time than the international media, although they later settled on an ambiguous combination of terrorism, Iran, and hacking. Exploring both local and international portrayals of cybersecurity incidents across languages enables a close analysis of this ambiguity.

[312] Muhammad Al-Ghamdi, 'Muhawalat Ikhtiraq ʾaramku Tahdufu Lil-ʾidrar Bil-Iqtisad Al-Watani Wa Manaʿa Tadaffuq Al-Zait ʾila Al-ʾaswaq Al-Mahaliyya Wa Al-ʿalamiyya [The Attempted Attack of Aramco Aims to Damage the National Economy and Stop the Flow of Oil to Local and Global Markets]', Al-Riyadh, 10 December 2012, https://perma.cc/55U5-RCFM.

[313] Staff Report, 'Hujum Khariji Istahdafa Shabakat Sharikat Aramku [External Attacks Target Aramco Company Networks]', Al-ʿArabiyya, 9 December 2012, https://perma.cc/6DRT-LZUJ.

[314] Staff Report, 'Aramku Alsaʿudiyya: Ikhtiraq Shabakatuna Al-ʾilitroniyya Biʾab Istahdaf Iqtisad Almamlika Wa Waqqafa Tadaffuq Al-Nuft Wa Al-Ghaz [Saudi Aramco: The Hack of Our Electronic Networks Was Aimed at the Kingdom's Economy and Stopping the Flow of Oil and Gas]', Al-Quds Al-ʿArabi, 9 December 2012, https://perma.cc/B46P-6R26.

[315] ʿAbd Al-Rahman Al-Rashid, 'Al-Hujum ʿala Aramku Wa Sad Niu Yurk [The Attacks on Aramco and a New York Dam]', Al-Sharq Al-ʾAwsat, 27 March 2016, https://perma.cc/K939-HEB9.

5.2.2 Shamoon 2

The name Shamoon was then given to a second incident that took place between November 2016 and February 2017. Unlike the first version, but like other campaigns explored later in this chapter, it was a series of incidents affecting different organisations with similarities in 'techniques, tactics, and procedures' (TTPs). In November 2016, malware with similar wiping functionality to Shamoon 1 was identified on the networks of multiple organisations in the Saudi government, including the central bank, and caused a temporary halt to operations at the Civil Aviation Authority. This malware, which resurfaced with minor changes throughout late 2016 and early 2017, was again attributed to the Iranian government.[316]

The technical characteristics of the 2016 malware clearly referenced the first Shamoon. The 2016 malware set the date on the infected computer to August 2012 (shortly before Shamoon 1 had begun to wipe data) and instructed the computer to wipe itself when the computer clock reached the time the first Shamoon occurred. This technical link, written *into* the malware by its authors, was both an overt claim of attribution (that the same actors were responsible for both incidents) and a sign of bravado (that these actors were able to infiltrate and wipe networks at any time). Furthermore, the malware used the same wiping mechanism as the first Shamoon and was also delivered through phishing emails, in which an unsuspecting user clicks on a link to download the malware.

Again, the marketing choices of the cybersecurity companies that analysed this malware helped establish an association with Shamoon 1. The 2016 incident was called "Shamoon 2.0" in Kaspersky's report, reinforcing the technical link between the two incidents above. However, this framing of the malware as a reoccurrence of the 2012 version was complicated by its technical analysis. Kaspersky identified yet another malware during their investigation of Shamoon 2, with both wiping and espionage functionalities, thereby complicating the idea of a single 'heir' to the

[316] Bill Gertz, 'Iran Renews Destructive Cyber Attacks on Saudi Arabia', *Washington Free Beacon* (blog), 22 February 2017, https://perma.cc/CBF9-XE9M; Michael Riley, Glen Carey, and John Fraher, 'Saudi Arabia Has Just Suffered a Series of Major Cyber Hack Attacks', *Bloomberg*, 1 December 2016, https://perma.cc/FRK8-AV2P.

2012 version.[317] Also, the Shamoon 2 malware had ransomware functionality, which indicated that it had been designed with the option to restore data after payment, rather than delete data irreversibly, and was therefore not 'destructive' in the same sense. Finally, the technical infrastructure around Shamoon 2 was associated with Iranian cyberespionage campaigns that had occurred earlier in 2017 by another cybersecurity company, FireEye.[318] In sum, Shamoon 2 was constructed as a 'reoccurrence' of Shamoon 1 by expert cybersecurity reports due to professional incentives, despite substantial ambiguity and the ready availability of other interpretations. This ambiguity ran deep in the professional discourse, as both the association with Shamoon 1 and the discrepancies could be supported by social and technical factors, including characteristics of the malware itself, expert judgement about its origin, and the surrounding technical infrastructure.

Shamoon 2 had a similar effect on professionals in the region, which I observed first-hand during my fieldwork. Saudi government officials left conferences I was attending mid-speech in November 2016, while interviewees showed me their latest analysis of the malware in near-real time. However, Shamoon 2 had different consequences for cybersecurity professionals in the organisations affected. At a conference in Riyadh a couple of months later, one Saudi professional observed that "3 CIOs [Chief Information Officers] of ministries have been fired, of the 6 ministries which were affected by Shamoon 2" (MECS2017). Others emphasised Saudi Arabia's quick national-level response, although with a caveat on the persistence of commercial incentives:

> The government of Saudi Arabia stepped in pretty fast, the Kingdom NCSC [National Cyber Security Centre] within a day had said to everyone, government entities, different sector companies, and CI [critical infrastructure. Once a company finds out, every single vendor they have goes and helps. And other vendors as well because you can sell technology. It is sad for vendors which are incumbent but good for others who were not, as you can say that our tech is better. We're all there to sell technology in the end! (I-48).

[317] Kaspersky Lab, 'From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond' (Kaspersky Lab Global Research and Analysis Team, 7 March 2017).
[318] Jacqueline O'Leary et al., 'Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware « Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware', FireEye, 20 September 2017, 33, https://perma.cc/V8SR-7KBD.

For this interviewee the immediate response to Shamoon 2 was markedly different to Shamoon 1, both in terms of improved government coordination and commercially motivated offers of assistance.

Another interviewee working in the Saudi government again emphasised the potential for espionage as well as data deletion: "Shamoon 2 could have taken data, it affected 10, 13 ministries, some didn't work for weeks. What stops him from taking data, if he can get onto every computer and boot a disk wiper?" (I-51). While Shamoon 1 highlighted an ambiguity between cybersecurity referents of business profits and critical infrastructure, Shamoon 2 contained an equally deep ambiguity between destruction and espionage.

Turning to the media reception, the Saudi online paper Sabq reported on Shamoon 2 very quickly after it occurred, with an article on 01 December 2016 summarising the complex links between the two Shamoons, as well as noting potential Iranian involvement.[319] This was a much quicker media response than for Shamoon 1, suggesting that the discursive space for talking about cyberattacks in the Saudi media had shifted dramatically in the intervening four years (partly due to developments in the Saudi government analysed in Chapter 7). However, the Arabic press generally was less responsive than Sabq: the next report was by Al-Jazeera six weeks later, making no attribution and repeating technical claims by cybersecurity company Palo Alto Networks.[320]

Many of the Saudi dailies began to report on Shamoon 2 at the same time as Al-Jazeera, suggesting some coordination in the Saudi media or at least a shared sense of competition with the Qatari outlet. Only two of these Saudi reports went beyond a simple repetition of the analysis of cybersecurity companies. The first, Al-Mowaten, reported on Shamoon 2 on 24 January 2017, describing it as destructive (*mudammir*).[321] Interestingly in light of the ambiguous espionage capability of Shamoon 2, Al-Mowaten reframed the original Shamoon 1 attacks, claiming that in

[319] Khalid ʿAli, 'Baʿad Ikhtifaʾ 4 Sanawat… 'shamʿun Yaʿudu Limuwajihat Al-Saʿudiyya [After Disappearing for 4 Years… Shamoon Returns to Confront Saudi Arabia]', Sabq, 1 December 2016, https://perma.cc/QK5T-8BHY.
[320] Staff Report, 'Rusida Mauja Thaniyya Min Hujumat Shamʿun 2 Bil-Saʿudiyya [Second Wave of Shamoon 2 Attacks Observed in Saudi Arabia]', Al-Jazeera, 17 January 2017, https://perma.cc/F9Z3-Q73P.
[321] Staff Report, 'Madha Taʿarifu ʿan Firus Shamʿun Al-Mudammir? [What Do You Know about the Destructive Shamoon Virus?]', Al-Mowaten, 24 January 2017, https://perma.cc/RJ7F-BQL9.

addition to the data deletion Shamoon 1 had achieved the 'theft of thousands of personal files' (*sariqat alʾaf al-milfat al-shakhsiyya*).[322] It also stressed that Shamoon 2 was a problem worldwide, and although Iran was associated with Shamoon 1 it could not confirm any link to Shamoon 2. Right-wing daily Okaz adopted a similarly cautious approach. Although it carried an interview with a US digital forensics expert under the title 'Iranian militias behind Shamoon' (*milishiyya ʾiraniyya waraʾ hujumat shamʿun*) just after the Al-Mowaten report, the interview merely traced the origin of the malware through the already public Iranian attribution of Shamoon 1 to the original US-Israeli Stuxnet operation, highlighting that it was unclear whether Shamoon 2 was a copy or development, and the author made no further claims beyond the provocative title.[323]

This analysis suggests that not only was the domestic media much more aligned with international media and cybersecurity companies than after the first Shamoon, but that the content and tone of the media coverage also changed. These reports were much less sensationalist and treated cybersecurity incidents as something that - although potentially destructive - was nonetheless fairly routine and could be mitigated with simple steps (some Saudi newspapers also gave advice on how to avoid infection).

Overall, Shamoon was *the* pivotal incident in the narrative of most cybersecurity professionals in the region and was the catalyst for the emergence of cybersecurity as a priority topic in the region for organisations in both public and private sectors. As both Shamoon incidents demonstrate that cybersecurity events are ambiguously constructed from both social and technical ingredients, as well as differing between regions, the importance of these events provided the impetus for the proliferation of this ambiguity throughout the professional discourse.

[322] Staff Report.
[323] ʾIbrahim ʿAqili, 'Milishiyya ʾiraniyya Waraʾ Hujumat Shamʿun [Iranian Militias behind Shamoon Attacks]', Okaz, 25 January 2017, https://perma.cc/753U-7WZB.

5.3 Proliferation

I now examine the proliferation of cybersecurity incidents in the region in the period 2011-2017. I treat these incidents in turn focusing on two categories used by cybersecurity professionals: cyber espionage and hacktivism. Following this, I synthesise data on all cybersecurity incidents in the region to demonstrate the first key plank of the thesis argument: that these categories are themselves ambiguous, fluid and interchangeable.

5.3.1 Cyber espionage

The first incident of cyberespionage in Egypt and the Gulf states was a campaign named Night Dragon in early 2011. Night Dragon was the codename given by cybersecurity company McAfee to a multi-year campaign against energy companies around the world, including in the Gulf states, in which widely available hacking tools were used to penetrate their computer networks, and, in some cases, remove data from industrial systems. This campaign was attributed by McAfee to actors based in China (with an oblique reference to this attribution in the name "Night Dragon"). The assumed motive was economic, as McAfee stated that "these attacks focus on the theft of specific data and intellectual property", aiming for "corporate and commercial targets".[324] The documents obtained by the espionage campaign also suggested an economic motive, as it took "sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations".[325] For McAfee, the wider lesson was clear: "miscreants continue to infiltrate networks and exfiltrate sensitive and proprietary data upon which the world's economies depend".[326]

However, Night Dragon also carried the possibility of other cybersecurity referents, as McAfee suggested that Night Dragon "speaks to quite a sad state of our critical infrastructure

[324] McAfee Labs, 'Global Energy Cyberattacks: "Night Dragon"' (McAfee, 10 February 2011), p.13.
[325] McAfee Labs, p.3.
[326] McAfee Labs, p.3.

security".[327] An expert comment on the McAfee report went further: "The threat of cyber terrorism is no longer a problem of the future… A targeted attack may cost companies dearly, both in terms of financial losses and productivity loss. The potential proceeds, for instance from extortion, are huge."[328] Here the risks demonstrated by a single cybersecurity incident were extremely ambiguous, from theft and damage to critical infrastructure to 'cyberterrorism'. The range of referents also increased over time: at the time of writing, McAfee's website claimed that "the tools and techniques behind Night Dragon are not specific to critical infrastructure and can be used to launch attacks against any industry."[329]

Cyberespionage then became a standard part of state intelligence capabilities worldwide, including in the region studies by this thesis. In 2012, US-designed malware called Flame was discovered on many networks including in Egypt and Saudi Arabia. Cybersecurity company Kaspersky assessed that Flame was built by the same organisations who created Stuxnet, and that it had been active since March 2010.[330] Another espionage tool similar to Flame, named Gauss, was identified by Kaspersky in 2012. Infections by Gauss throughout 2011 and 2012 were mainly in Lebanon, although fewer instances were across the Levant and Gulf.[331] Two years later, sophisticated malware named REGIN was discovered by cybersecurity companies on a wide range of organisations worldwide. According to Symantec, 24% of infections were in Saudi Arabia, the second-highest single state (after Russia with 28%).[332] Following the Snowden disclosures the year before, this malware was linked to the Five Eyes intelligence community (UK, US, Australia, Canada, New Zealand), and specifically the UK and US signals intelligence agencies GCHQ and

[327] Diane Bartz, 'Chinese Hackers Infiltrated Five Energy Firms: McAfee', Reuters, 10 February 2011, https://perma.cc/75A3-TZTU.
[328] Dan Raywood, 'McAfee CTO Warns of New Combined Threat Named "Night Dragon"', SC Media UK, 10 February 2011, https://perma.cc/QZY5-293P.
[329] McAfee Labs, 'Night Dragon', McAfee, accessed 16 January 2018, https://perma.cc/GLD2-BJ9N.
[330] Alexander Gostev, 'The Flame: Questions and Answers', Securelist GREAT (Kaspersky Lab), 28 May 2012, https://perma.cc/8Z47-U5MW.
[331] Kaspersky Lab, 'Gauss: Abnormal Distribution' (Kaspersky Lab Global Research and Analysis Group, 9 August 2012).
[332] Symantec Security Response, 'Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance', 24 November 2014.

NSA.[333] Separately, cyber-espionage operations attributed to Iran have been conducted against targets in the US, Europe, and in the Middle East since 2011.

These 'cyber powers' were not the only actors involved in interstate competition using cyber tools. Another campaign, named Desert Falcons by Kaspersky Lab, was claimed to be "the first known cyberespionage attacks to be fully developed and operated by Arabic speakers to target the Middle East."[334] The actors used infrastructure in Egypt, Palestine, and Turkey, and had a wide range of targets, although the most concentrated instances were in Egypt, Israel and Palestine. The Desert Falcons campaign was never attributed with confidence to a specific state.

The lines between state cyber espionage, individual actions, and even the investigations carried out by cybersecurity companies blur extensively. A good example is an actor identified as 'Molerats' by cybersecurity companies, who used Arabic language documents to construct phishing emails in late 2011, suggesting targets in the Palestinian territories.[335] However, in 2012, the same actor used a remote access tool (RAT) from a Gaza-based IP address to infiltrate the Israeli police force.[336] In 2013, the same actor then switched to a different tool, named Poison Ivy, which was commonly associated with Chinese cyber espionage at that time.[337] Incidents associated with this actor in 2015 were mainly targeted at Egypt, the UAE, and Yemen,[338] but also the Middle East more widely.[339] This complex trail of events, linked through technical details and expert assessments, is difficult to categorise and highly ambiguous.

The attribution of Molerats to a specific individual or organisation is similarly ambiguous. One report associated these events with a group named Gaza Hackers Team (*fariq qarasina ghaza*),

---

[333] Marcel Rosenbach, Hilmar Schmundt, and Christian Stöcker, 'Source Code Similarities: Experts Unmask "Regin" Trojan as NSA Tool', *Spiegel Online*, 27 January 2015, https://perma.cc/SEH5-YA94.
[334] Kaspersky Lab, 'The Desert Falcons Targeted Attacks', Securelist - GREAT, 17 February 2015, https://perma.cc/BE9U-3NG5.
[335] Nart Villeneuve, 'New Xtreme RAT Attacks US, Israel, and Other Foreign Governments', TrendLabs Security Intelligence Blog, 14 November 2012, https://perma.cc/R5GC-7FAB.
[336] Brian Krebs, 'Malware Spy Network Targeted Israelis, Palestinians', *Krebs on Security* (blog), 12 November 2012, https://perma.cc/4NJT-F2SZ.
[337] Nart Villeneuve, Thoufique Haq, and Ned Moran, 'Operation Molerats: Middle East Cyber Attacks Using Poison Ivy', FireEye, 23 August 2013, https://perma.cc/6UJT-WKZ2.
[338] Tom Lancaster, 'Attacks against Israeli & Palestinian Interests - Cyber Security Updates', 27 April 2015, https://perma.cc/4W4T-BAHZ; Kaspersky Lab, 'Gaza Cybergang, Where's Your IR Team?', Securelist - GREAT, 28 September 2015, https://perma.cc/B65T-WHKL.
[339] Clearsky, 'Operation Dusty Sky', January 2016, clearskysec.com/dustysky.

which appeared to be run from Algeria. Strikingly, another cybersecurity company tracking this actor received emails from someone they assessed to be the actor themselves (from a fake account) asking for the information the company held about that individual. The company reported that they "did not send any information to the attackers. However, we used the new leads to deepen the investigation".[340] Although their latest report attributes these incidents to Hamas, the conversation between the company and the actor suggests that it was a single individual using a Gaza-based IP address. Lastly, this reciprocal contact between 'investigators' and 'attackers' is reminiscent of espionage and intelligence work more widely, highlighting the overlap with expert practices in intelligence noted in the previous chapter.

Despite this overall ambiguity, some incidents were simply characterised as commercial rather than state espionage. In 2014, malware was detected that was specifically designed to remove data from energy companies, with most of its instances in the Gulf states (25% in the UAE alone).[341] Similar commercial espionage also occurred in the finance sector in 2016, when phishing emails were sent to a wide range of organisations, predominantly in the Middle East, appearing to be from UAE bank EmiratesNBD.[342] The motivation was reported to be purely commercial espionage, as these emails were sent to senior executives in large private organisations. Not all cybersecurity incidents therefore offer the same level of ambiguity between referents as those detailed above.

5.3.2 Hacktivism

Politically motivated incidents in cybersecurity span a large range of activity, from 'hacktivism' (such as the Gaza Hackers Team above) and so-called 'cyberterrorism'. Although scholars have attempted to both define and deflate the concept of cyberterrorism,[343] the distinction

[340] Clearsky, 'Operation Dusty Sky Part 2', June 2016, www.clearskysec.com/dustysky2.
[341] Christian Tripputi, 'New Reconnaissance Threat Trojan.Laziok Targets the Energy Sector', Symantec Security Response, 30 March 2015, https://perma.cc/Z6NW-M6U9.
[342] Mohamad Amin Hasbini, 'Operation Ghoul: Targeted Attacks on Industrial and Engineering Organizations', Securelist - GREAT (Kaspersky Lab), 17 August 2016, https://perma.cc/TEF3-VW3L.
[343] Lee Jarvis, Stuart Macdonald, and Lella Nouri, 'The Cyberterrorism Threat: Findings from a Survey of Researchers', *Studies in Conflict & Terrorism* 37, no. 1 (2 January 2014): 68–90.

between the two is often deliberately muddied by the actors themselves. For example, in 2012, individuals claiming affiliation with a Saudi hacking group called 'group-xp' obtained 400,000 credit card accounts from an Israeli sports website; in retaliation, an individual claiming to be an Israeli soldier posted personal information of Saudis, Egyptians, and others online. Then, the websites for the national Israeli airline, stock exchange, and three banks were taken offline, probably by group-xp.[344] The motive for this 'group', which was in fact a 19-year old Saudi citizen, was explored in an online chat with a journalist after this incident.[345] When asked "would you call what you're doing hacktivism? Or cyberterrorism?", his response was "could be anything. I just want to see Israel suffer". When asked again for his motive, he explained that "Israel kills Israeli innocent people, it's what their government do, it's their daily business, they do not obey any law, international law, so I want to harm them in ANY way I can". Hacktivism and cyberterrorism are thus ambiguous terms, especially for the actors involved.

Others have embraced both labels to create publicity, and in some cases, distract attribution efforts. A range of groups claiming affiliation with Islamic State conducted cyber operations in 2015 and 2016, including under the labels "Cyber Caliphate" and "Islamic Cyber Army". As well as defacing websites, one of their tactics was to release personal information of government employees in countries fighting them in the Syrian conflict; for example, the Saudi Royal Guard.[346] While some individuals operating from ISIS-held territory in Syria were engaged in online recruitment and other 'cyber' activities, other operations claimed by the 'Cyber Caliphate' were later attributed to Russian intelligence agencies using a 'false flag' to prevent discovery.[347] These discoveries blur the lines not only between hacktivism and cyberterrorism, but also between cyberterrorism and cyber espionage. The unclear distinctions between hacktivism and cyberterrorism meant that other hacktivists took pains to distance themselves from terrorist labels. In 2014, a group called Cyber of Emotion obtained

[344] Nick Enoch, 'Hamas Hails Hack Attack against Websites of Israel's Stock Exchange, El Al Airline and Three Banks', Mail Online, 16 January 2012, https://perma.cc/B4UK-G9Q3.
[345] Adrian Chen, 'A Chat With the Teen Saudi Hacker Who Says He Stole a Million Israeli Credit Cards', Gawker, 6 January 2012, https://perma.cc/9WT9-7LCH.
[346] Laith Alkhouri, Alex Kassirer, and Allison Nixon, 'Hacking for ISIS: The Emergent Cyber Threat Landscape' (Flashpoint, 2016).
[347] Ian Allen, 'Islamic State's Online Army Is a Russian Front, Says German Intelligence', intelnews.org, 20 June 2016, https://perma.cc/QMG4-UKJ7.

access to the Twitter account of the Saudi Ministry of Justice and highlighted a supposed $45 million cost for website development.[348] In August 2015 the same group then took other Saudi government websites offline, claiming to demonstrate the security vulnerabilities in government systems. This group left messages saying "We do not want to harm the site. Had it been hacked by enemies, your personal information, emails and registration data would have been compromised." This group deliberately distinguished their political motivation from more radical opposition to the Saudi government to avoid the label of cyberterrorism.

Other hacktivist groups mobilised in support of domestic political issues in the region. In 2015, hacktivist collective Anonymous launched "OpNIMR". OpNIMR was named after Ali Al-Nimr, the nephew of dissident leader Sheikh Nimr Al-Nimr, who was imprisoned in 2012 following his participation in pro-democracy protests and later sentenced to death. OpNIMR was a distributed denial of service (DDOS) attack, which aimed to send a massive number of requests to websites of Saudi government and foreign embassies and thereby take them offline.[349] The Anonymous operation continued after the execution of Sheikh Nimr Al-Nimr in January 2016 in a series of executions drawing widespread international criticism. Their motivation was made clear in an interview with one of the coordinators of the operation, who explained that:

> I think it's because he [Ali Al-Nimr] is so young. He's all about anti-government protests and we're totally against the government, so really he was doing us a favor and now we are doing him a favor… It was also a social media trend at the time and we thought we'd do something about it. Saudi Arabia has been approved to be on the UN Human Rights Council. They're crucifying and beheading a 21-year-old - do you really want them to be in front of Human Rights at the UN? In addition to already having executed 127 people this year? It's not right.[350]

From the perspective of cybersecurity professionals, this incident subverts the usual categories of threat and victim. While Anonymous are usually considered a classic 'hacktivist' cybersecurity threat, and US-based cybersecurity companies assisted the Saudi government in many of the cases

[348] Al-Jazeera, 'Saudi Websites Hacked by "Well-Intentioned" Group', 15 August 2015, https://perma.cc/JKK3-M75B.
[349] David Gilbert, 'Anonymous Knocks Saudi Government Websites Offline In Protest Against Planned Beheading And Crucifixion Of Ali Mohammad Baqir Al-Nimr', International Business Times, 28 September 2015, https://perma.cc/6Q8Y-4DVN.
[350] Carl Nasman, 'Anonymous Hacktivist Explains Why Group Is Targeting Saudi Arabian Government', DW.COM, 2 October 2015, https://perma.cc/WQ3Z-FZX6.

above, here influential cybersecurity professionals in the US supported Anonymous.[351] Their position thereby became the exact opposite of the local media, who usually relied on their analysis (for example in the Shamoon incidents in the previous section). For example, Anonymous was placed neatly into the Saudi media's existing set of cybersecurity threats, as the right-wing Saudi paper Okaz labelled Anonymous as a 'terrorist hacker' (*hakar ʾirhabi*) and blamed the operation on the support of the 'digital Satan Iran' (*al-shaitan al-raqmi ʾiran*).[352] As well as illuminating ambiguities in the conception of cybersecurity between cybersecurity professionals and their clients, this incident also anticipates the introduction of human rights into cybersecurity considered in Part 2.

5.3.3 Synthesis

The overarching theme of all the cybersecurity incidents considered in this chapter is that their interpretation is complex, requiring significant expertise and containing vast areas of ambiguity and uncertainty. Consequently, they simultaneously support several varied categorisations, the salience of which shifts over time. To illustrate the flexible construction of cybersecurity incidents in Egypt and the Gulf states, I distinguished four categories: hacktivism (as above), cyberespionage (as above), cybercrime (as in the Phish Phry and Bank Muscat scams in the first section of this chapter), and critical infrastructure attacks (as in the two Shamoons). I then catalogued all key events within these four categories, including but not limited to the ones discussed in this chapter, noting how far they supported multiple interpretations. The result is displayed in Figure 3.

[351] Pierluigi Paganini, '#OpNimr Anonymous Targets Saudi Websites to Stop Al-Nimr's Crucifixion', Security Affairs, 28 September 2015, https://perma.cc/F42P-SK3J.
[352] ʿAbd Al-Razzaq Al-Marjan, 'ʾiran Taqudu Shaghaban Raqmian Litashjiʿ Al-ʿunf [Iran Leads Digital Subversion to Encourage Violence]', Okaz, 5 January 2016, https://perma.cc/KAN4-LHW7.

Figure 3: Cybersecurity events in Egypt and the GCC, 2011-2017

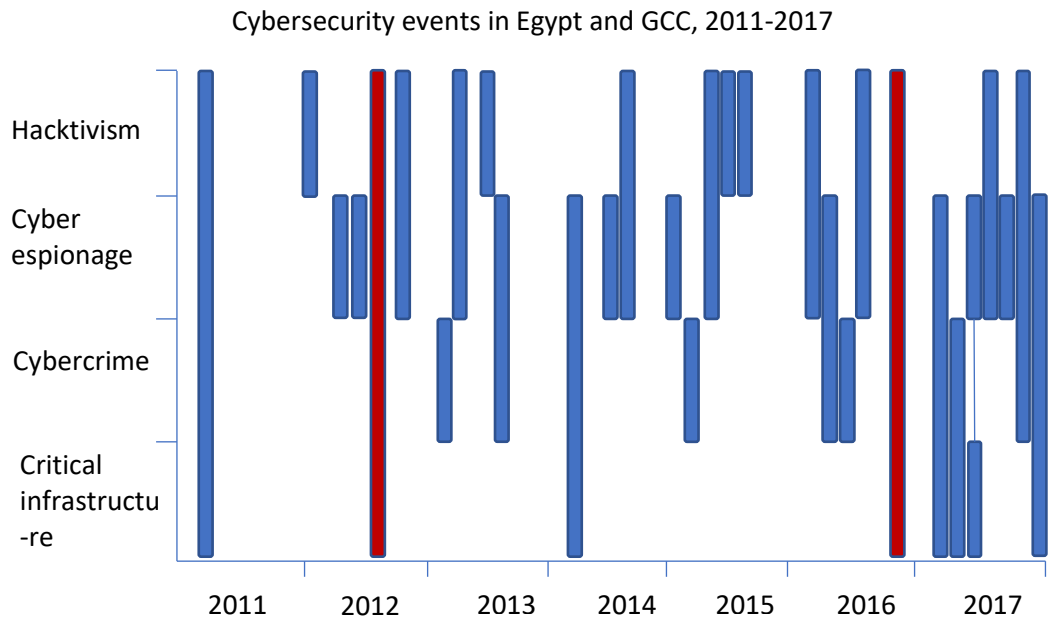


Figure 3 provides an indication of the increasing frequency of cybersecurity incidents in Egypt and the Gulf states in the period examined by this thesis, with Shamoon 1 and 2 in red.[353] This increase is unsurprising and could likely be replicated worldwide. More importantly, it also shows that over half (18 of 30 incidents) were associated with multiple categories, suggesting that all four categories were deployed flexibly by cybersecurity experts to interpret key events, moving smoothly between diverse frames. The influence of these categories is not limited to the construction of threat actors. The organisations targeted by these actors are also constructed differently. Both states and companies can be seen as providers of critical infrastructure, as generating and reacting to political opposition, or as equal participants in cyber espionage.

Nonetheless, there is an overarching framework into which these categories fit, which returns us to the fundamental structure of the professional cybersecurity discourse itself. The threat is an unknown, shadowy actor, often described simply as 'malicious'. The victim is nearly always an organisation, whether public or private. This frame was only subverted by the Anonymous

[353] Its analysis requires one caveat: the time of an event is assumed to be the date of the report release on an incident. Many incidents extend over a substantial period and reports are often described as 'campaigns', focusing on a single group over time.

incident considered above. Together, I describe this overarching framework as an 'organisational' cluster of values, combining different values implied by espionage, hacktivism, crime and war into a conception of cybersecurity that treats organisations as the chief repositories of value, and threats to those organisations as the main cybersecurity threats. These values are clustered due to technological characteristics, institutional mechanics and prevailing interests.

This overarching frame has two specific benefits for cybersecurity companies. First, it hides the difficulties these companies face in extracting a clear narrative from a mass of technical detail. Second, its ambiguity is *productive.* As cybersecurity companies are essentially commercial entities (although often aligned with states and adopting their security culture), the frame of 'malicious actor' and 'victim organisation' enables cybersecurity companies to read events as demonstrating cybersecurity risks to a wider range of potential clients than any individual category. Thus the commercial interests of cybersecurity experts themselves play a part in creating this ambiguous professional discourse.

Finally, there is a clear sense of the reports themselves coalescing into a specific structure. Nearly all the cybersecurity reports analysed follow repetitive and highly structured formats, providing 'indicators of compromise' and other technical details of the malicious actor to enable others in the community to work on the same problem. These formats are also designed for easy branding and marketing, using slick graphics and catchy codenames to cohere a disparate mass of information into an easily digestible narrative. These reports are also strategic tools, as cybersecurity companies use the response by threat actors to their public reports to obtain new data. These characteristics will reappear in the next chapter, as I analyse how NGOs aligned human rights values with the dominant conceptions of cybersecurity considered here.

PART 2: MORAL MANOEUVRES

Chapter 6: Alignment

A single UAE citizen named Ahmed Mansoor has been targeted by at least three separate types of surveillance software, probably purchased by the UAE government. He has also been subject to mistreatment and arbitrary detention by the same government. The most sophisticated of the three types of surveillance software, made by Israeli company NSO Group, was located on Mansoor's devices in 2016 after a collaboration between Citizen Lab, an NGO focusing on human rights and internet technologies, and Lookout, a mobile phone cybersecurity company. They released a report snappily titled 'The Million Dollar Dissident', due to the combined price of the three sets of surveillance equipment. This report had extensive technical details of the NSO Group software and how it had been detected. I argue in this chapter that this was part of the moral manoeuvre of *alignment*: these actors aligned human rights values with what I call organisational values in cybersecurity, including the discursive characteristics of threat reports, for an invested reason: to draw attention to Mansoor's predicament.

This chapter argues that the moral manoeuvre of alignment – altering the values and technical claims of cybersecurity in ways that mirror existing value clusters - provides a better explanation of this phenomenon than approaches that focus solely on norm entrepreneurs and transnational advocacy networks. This is because alignment highlights how some human rights actors consciously reject the position of other civil society human rights advocates and engage in wider normative debate with opponents outside the specific issue of human rights violations.

This chapter is structured in three sections. The first section details the relationship of the regional cybersecurity professional community to human rights. The second section details the role of other cybersecurity experts, such as Citizen Lab, in associating surveillance technologies with human rights violations. The third section explores the amendment of the Wassenaar Arrangement to include these technologies.

6.1 Regional cybersecurity professionals

This section argues that this professional community largely avoided engagement with human rights values, and so alignment was performed by cybersecurity experts *outside* this community. As outlined in Chapter 3, the events in 2011 known as the Arab Spring were widely portrayed as a watershed moment for human rights values in the Middle East, and so this is a good starting point from which to investigate the views of human rights held by the regional cybersecurity professional community.

Some interviewees adopted the narrative of incumbent governments about the Arab Spring events, linking cybersecurity to questions of national stability and the maintenance of societal functions throughout periods of protest and revolution. For example, a UK national working in the Gulf summarised his perspective as follows:

> Within the region, look at Aramco, and the Arab Spring. Countries are not brought down by terrorism, they are brought down through civil disorder… Anywhere in the region the big concern is for cyber to damage heavy economics. Take 9/11: no nation state collapses from a terrorist attack. Countries fall due to their population not being happy, critical services not being there, not being able to take cash out. Population growth, austerity, religious perspectives, all these are added to by cyber. It could create another Arab Spring if CNI [critical national infrastructure], heavy handedness by Police, and everything comes out. Regionally it is a wide worry (I-46).

This interviewee understood 'cyber' issues as adding to existing tensions contributing to the events of the Arab Spring. Although their description of some of these tensions (e.g. 'heavy handedness') could be framed in terms of human rights, this interviewee instead saw the main cybersecurity risks as being directly to organisations such as banks and governments and then indirectly to society more widely. This interviewee thus used the example of the Arab Spring to reinforce the organisational cluster of values outlined in the previous chapter, rather than import human rights values into cybersecurity.

Another interviewee, based in the UK with regular travel to the region, characterised the Arab Spring in a similar manner:

> The effects of mass communications – observe the Arab Spring. All countries [in the Middle East] are characterised by governments of authority and inherited leadership, with legitimacy through accessibility and direct complaints every Friday. In Dubai in

> the 50s and 60s, and in the funny little emirates around it, you would petition the ruler, that's how they had legitimacy (they had it other ways as well). But now there has been a flood of activity – a peaceful country can ferment in 12 hours. Even biddable, contented Oman had protests. We need to think about the use of cyber tools to draw out data from sources which previously had integrity (I-30).

The logic of this quotation is worth unpacking. It moves from the Arab Spring to an abridged political history of the Gulf with a heavy dose of colonial paternalism, and then directly onto the implications for cybersecurity, especially the dangers of 'cyber tools'. It suggests that cybersecurity professionals combine their technical expertise with a particular regional imaginary in order to form their judgement of cybersecurity risks. Interestingly, this interviewee then went on to connect this image of the region to the sale of cybersecurity technologies:

> The UK government has been very keen to promote UK solutions, as we are perceived as a thought leader in technology and in applications of technology – for example, in the security services. The debate that we have between using data to protect lives and privacy is very interesting for them [Middle East governments]. In times of unrest the offside line moves very far to the right, even here (I-30).

This interviewee here viewed the Arab Spring as an opportunity for commercial advantage and political influence in cybersecurity and surveillance (considered further in Chapter 8). The implication of their 'offside line' metaphor is that the UK would do exactly the same as the Middle East governments in situations of 'unrest', including limiting human rights values of freedom of expression and privacy. Overall, this interviewee saw the values defining the offside line as flexible and amorphous, requiring interpretation in specific circumstances and issues.

Other cybersecurity professionals echoed this point. As a conference presenter working as a consultant in the Saudi government said: "Mostly, privacy is what we say it is going to be, especially when you have security investment in this country and things need to be secure." (MECS2017). Here the presenter highlights the way cybersecurity experts can exercise their technical capacity to *define* human rights values like privacy in the building of databases and IT systems. This view of values as being substantiated or given meaning by technical claims is an important aspect of the self-image of the cybersecurity expert community.

Some cybersecurity professionals took a more direct approach to the Arab Spring. One presenter, a Saudi national, put up a famous picture of Egyptian protester Wael Ghoneim speaking

in January 2011 at a cybersecurity conference in Saudi Arabia in March 2017, with the following comment.

> Do you recognise this man? Do we like him? Not really. He is Wael Ghoneim, he brought the revolution to Egypt, and they called it the Facebook revolution. People were thankful at the time! But this is a very important dimension, and we need to think about the social dimension in information security (MECS2017).

The inclusion of this picture itself highlights the salience of the Arab Spring and the subsequent political turmoil in Egypt for cybersecurity. However, with the careful statement only that "people were thankful at the time" this presenter avoided any endorsement of the January 2011 revolution itself, and instead gave clear cues to their audience about the position they were expected to take. In asking the question 'do we like him?' this presenter implied that the regional professional community should judge the legitimacy of the protests only *as cybersecurity professionals*. The answer given by the presenter resonates with the interviews above, suggesting that cybersecurity professionals do not 'like' Ghoneim because they seek to maintain stability.

After this presentation, I had a conversation with the presenter in which I asked why he categorised both the Egypt revolution and the Shamoon incident (inevitably, another central point in his presentation) as cybersecurity threats. He replied "If we fail to connect them, we are subject to greater risks. We need to connect the dots… Some people segregate infosec [information security] and safety, but I have brought them together, over time they will be more connected". By bringing the Egyptian revolution into the range of cybersecurity threats considered in the previous chapter, this presenter places it firmly within the organisational cluster of values structuring those threats. This definition of the Arab Spring bypasses human rights interpretations altogether.

In contrast, other conference presenters raised human rights issues, but in a very tentative way. One example is a presentation by Marco Gercke, the head of ITU-IMPACT, at the Arab Region Cybersecurity Summit in 2016. In this presentation, Gercke introduced a 'hypothetical' case study where Anonymous launched a cyberattack against an Arab government because they "don't like your human rights violations" (ARCS2016). As seen in Chapter 5, this is based on an actual incident: the 2012 Anonymous OpNIMR was explicitly linked to the execution of opposition figures in Saudi Arabia and its poor human rights record. This was a rare mention of the phrase 'human rights

violations' in the conferences I attended, and his explanation of this case study was followed by an uncomfortable silence in the audience. This unease was manifest even though Gercke presented human rights values as a motivation for cybersecurity *threat actors*, rather than as a central concern for cybersecurity professionals.

Gercke seemed to sense this unease and quickly qualified his hypothetical case study, saying that "come on, in any country we can find someone like that". By adding this qualification, he implied that human rights values were merely a source of rhetoric for those opposing the government, diminishing their relevance to cybersecurity. This directly contradicts the cybersecurity professionals based in US and Europe noted in the previous chapter who supported OpNIMR.

An interviewee working in the Saudi government at the time of the OpNIMR incident echoed Gercke's view of Anonymous, saying that:

> The Anonymous thing was because of persecution, or claimed persecution. For me, it's the same, all of them. They are just getting into my networks, damaging my networks. Maybe the intention might be different, and for someone higher up in government this might be important, but for me it's the same (I-51).

This interviewee not only presented human rights values (i.e. 'claimed persecution') as a motivation for threat actors, rather than a relevant value for cybersecurity professionals themselves, but also emphasised that this was outside his *professional* remit, which concentrated on the protection of networks. Differences in adversary motivations were a matter for others outside the profession.

Overall, as this analysis has indicated, most of the cybersecurity professional community saw cybersecurity as at least separate from human rights issues, and at most opposed to them. However, the community itself contains a variety of viewpoints, and some conference presenters *did* see human rights as part of their professional identity. As one Egyptian conference presenter explained to me in a conversation after their presentation:

> After the revolution it was about information leakage, about individuals who were against the government, who would then face real threats if their information went online. And it was the security teams who were doing it. So this was an ethical reason, not a commercial one, to do cybersecurity (CSC2016).

Similarly, another recognised that "lots of this technology could be used for bad purposes, so the ethical concerns are important" (CSC2016). Both these professionals saw cybersecurity, in the

context of the January 2011 revolution, as centrally concerned with the security of individuals rather than organisations. Finally, a few cybersecurity professionals included human rights values, especially privacy and freedom of expression, as part of a wider range of values relevant to cybersecurity. For example, an Egyptian interviewee characterised the political debate in Egypt:

> People are flipping from one side to the other, do they want more security or privacy, there is a choice between these. Interesting times over the last 5-6 years, with the Snowden effect. There are four goals: security, privacy, transparency, and freedom of expression. 100% of any of these is not achievable, and we need to make the right compromises. These are four different groups that don't usually overlap, and you need to create common ground. Maybe freedom of expression is the easiest to isolate, but you need to have a bridge (I-24).

This quotation identifies four values as relevant for cybersecurity, only one of which is the organisational cluster of values explored in the previous chapter (under the heading of 'security'). This interviewee sees the crucial task of cybersecurity as bringing these values together on common ground or building a bridge. This, I suggest, is the beginnings of the moral manoeuvre of alignment. However, as this section has demonstrated that many cybersecurity professionals in the regional community do not seek an alignment between organisational and rights-based versions of cybersecurity, I now examine experts outside this community who have done exactly that.

6.2 Human rights and cybersecurity

Many human rights are potentially relevant to cybersecurity, and the 'hacker' community that preceded contemporary cybersecurity professionals had a strongly libertarian ethos based on inalienable individual rights.[354] The UN Human Rights Council connected human rights to actions on the internet when it stated in 2012 that:

> The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR).[355]

[354] E. Gabriella Coleman and Alex Golub, 'Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism', *Anthropological Theory* 8, no. 3 (1 September 2008): 255–77; Helen Nissenbaum, 'Hackers and the Contested Ontology of Cyberspace', *New Media & Society* 6, no. 2 (1 April 2004): 195–217.
[355] Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (United Nations General Assembly, A/HRC/RES/20/8, 16 July 2012).

In this section, I provide an overview of cases where human rights violations have been associated with surveillance technologies. The extent to which such technologies are 'cybersecurity' technologies or deserve inclusion in the issue area of cybersecurity is a crucial question, and is treated in detail in the third section of this chapter. This section is largely based on the work of international NGOs invested in the promotion of human rights, including the OpenNet Initiative, Privacy International, the Electronic Frontier Foundation (EFF), Citizen Lab and other researchers, journalists and activist groups such as Bahrain Watch. In particular, Citizen Lab, an interdisciplinary organisation based at the University of Toronto, has played a large role in interpreting human rights values in cybersecurity. Citizen Lab is led by an IR academic, Ron Deibert, whose theoretical work I considered in Chapter 2.

I follow the NGOs above in focusing specifically on two sets of rights: civil and political rights of freedom of expression and privacy, and rights prohibiting arbitrary detention and torture and mistreatment. These two sets of rights overlap significantly: detention and torture can be a means to stifle free expression, while restrictions on freedom of expression can lead to detention and mistreatment for individuals who overstep these boundaries. This focus puts aside not only all social and economic rights but also the civil and political rights of equality and political participation often examined in connection with the Middle East; by doing so I do not mean to imply that these other rights are less important. Also, as stated in Chapter 3, the ICCPR has not been signed or ratified by Saudi Arabia, Oman, Qatar or the UAE, although it nonetheless has the status of customary international law.

6.2.1 Violations in Egypt and the Gulf states

The technologies identified by NGOs include filtering, censorship and mass surveillance on one hand, and targeted surveillance on the other. I consider them in turn in this section. These examples are central to the moral manoeuvre of alignment, as they form the basis for a rights-based approach to cybersecurity.

Internet filtering and mass surveillance require technologies that can access and classify internet traffic on a large scale and on a very granular level – that of the data packets themselves, known as deep packet inspection (DPI).[356] DPI can be used for several purposes: to extract data associated with individuals (such as email addresses), to identify websites (by domain names such as www[dot]google[dot]com or by IP address), or to identify types of communication (e.g. voice over IP (VOIP)). While DPI has many other functions - such as improving the speed, quality, or cost of internet traffic – at a large scale it can be used for surveillance (gathering information about an individual or group) or filtering (blocking access to websites, blocking a type of internet communication by class (e.g. VOIP) or by product (e.g. Whatsapp)).

Of the states examined in this thesis, the first states where filtering technology was identified were those most affected by protests in the Arab Spring: Egypt and Bahrain. By 2009, Egypt already possessed precursors to DPI technology that allowed large scale access to telephone networks, provided by the company Nokia Siemens Networks (NSN).[357] In 2011, in the wake of international media attention on the Arab Spring, many media outlets ran stories on the use of surveillance by Arab Spring governments. For example, the Huffington Post reported that the Egyptian government used DPI-based monitoring technologies produced by an Israeli-origin subsidiary of Boeing, Narus.[358] Later in 2011, Bloomberg reported that surveillance technologies provided by NSN and Trovicor (a related company) were also used in Bahrain.[359] These technologies were reportedly the source of information on the basis of which activists were arrested and beaten.[360] The context of the Arab Spring facilitated the portrayal of such technologies as a threat to human rights.

Citizen Lab's work built on these initial reports, as they had already analysed filtering technologies worldwide for several years prior to the Arab Spring, and, like other NGOs, focused on

[356] Mass surveillance is a contested term, and intelligence agencies call the same activity 'bulk data collection'. Both terms have misleading connotations, and I use mass surveillance simply for ease of exposition, to distinguish it from targeted surveillance.
[357] Privacy International, 'The President's Men?', February 2016., p.13.
[358] Timothy Karr, 'One U.S. Corporation's Role in Egypt's Brutal Crackdown', Huffington Post, 28 January 2011, https://perma.cc/2KR6-D86Q.
[359] Privacy International, 'The President's Men?', p.13.
[360] Vernon Silver and Ben Elgin, 'Torture in Bahrain Becomes Routine with Help from Nokia Siemens', *Bloomberg*, 23 November 2011, https://perma.cc/WT2A-XTRF.

the Arab world in 2011. Their investigations revealed that all GCC states other than Oman used commercial filtering technologies at a national level. Specifically, Citizen Lab reported in 2011 that Canadian company Netsweeper provided DPI-based filtering technology to the UAE, Qatar and Kuwait (with Bahrain added in 2016).[361] They also detected that US company Blue Coat had DPI-based filtering and surveillance devices present in Egypt and all GCC countries other than Oman by January 2013.[362] Blue Coat had already been the subject of human rights criticism due to its sales elsewhere in the region, as Citizen Lab researchers had discovered in 2011 that Blue Coat devices had been sold via a UAE reseller to Syria.[363] Finally, McAfee's Smartfilter was identified by Citizen Lab in the UAE and Saudi Arabia later in 2013.[364] These reports together demonstrated that commercial filtering technologies were used by governments throughout the Gulf. They argued that these filtering services contravene the right of freedom of expression by blocking political opposition and civil society websites, as well as censorship on grounds of religion and decency.

Following worldwide recognition of mass surveillance after the Snowden disclosures in 2013, NGOs and media outlets revealed the use of DPI-based technologies by governments in Egypt and the Gulf states for surveillance as well as filtering. For example, a report on the French news site Telerama traced a relationship between Egypt, the UAE, and a French company named Amesys. This report claimed that in late 2013 and early 2014, part of the UAE's assistance to Egypt in support of the new military leadership and later President Al-Sisi was a DPI-based monitoring system produced by Amesys costing 10 million euros.[365] Its purpose was reportedly to monitor members of the Muslim Brotherhood. As detailed in Chapter 3, the Muslim Brotherhood and associated groups were subject to severe repression during this time following massacres of Brotherhood supporters in 2013.

---

[361] Jakub Dalek et al., 'Tender Confirmed, Rights at Risk: Verifying Netsweeper in Bahrain' (Citizen Lab, 21 September 2016); Nicki Thomas and and Amy Dempsey, 'Guelph-Based Software Censors the Internet in the Middle East', *The Toronto Star*, 13 June 2011, https://perma.cc/KH8H-KXPT.

[362] Morgan Marquis-Boire et al., 'Planet Blue Coat: Mapping Global Surveillance and Censorship Tools' (Citizen Lab, January 2013).

[363] Jakub Dalek and Adam Senft, 'Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma' (Citizen Lab, 9 November 2011), https://perma.cc/9X4U-FCQH.

[364] Bennett Haselton, 'Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE' (Citizen Lab, 28 November 2013).

[365] Olivier Tesquet, 'Amesys: Egyptian Trials and Tribulations of a French Digital Arms Dealer', Telerama, 5 July 2017, https://perma.cc/L288-BMJN.

Other media reports suggested that, later in 2014, Blue Coat's local subsidiary, a company named See Egypt,[366] had beaten Narus and Gamma International in a competition for monitoring contracts.[367] DPI devices made by Sweden-based and US-owned company Procera Networks (later called Sandvine) were also identified in Egypt in 2016. Although Procera Networks claimed its technologies were used solely for traffic management,[368] an analysis of these devices in situ by Citizen Lab in 2018 identified a range of other uses, including blocking websites and serving unwanted advertisements to internet users.[369] Finally, a BBC investigation in 2017 reported that Danish company ETI, acquired by BAE Systems in 2010, had sold national-level surveillance technologies to Saudi Arabia, UAE, Qatar, and Oman.[370] All these reports highlighted human rights violations committed by these governments, often by the same organisations that purchased and deployed the surveillance technologies.

I now turn to NGO and media reports on targeted surveillance software. These are systems that enable third-party access to specific devices, without the knowledge or permission of the user of that device, and which aim to avoid countermeasures aimed at preventing such access, with the ultimate purpose of extracting a wide range of information about and on that device. It is worth noting, although it does not affect the examples below, that DPI can also be integrated into targeted surveillance technologies by providing them with an additional vector of infection at the network level, rather than the vector most commonly used by the companies below, which is phishing links sent directly to the target.

A simple example of targeted surveillance is the use of software in Bahrain in 2011 and 2012 that revealed the IP address of at least 120 social media users by sending them an apparently

[366] Sheera Frenkel, 'U.S. Company Distances Itself From Egyptian Surveillance System', BuzzFeed, 18 September 2014, https://perma.cc/7TUF-CDZH.
[367] Maged Atef and Sheera Frenkel, 'Egypt Begins Surveillance Of Facebook, Twitter, And Skype On Unprecedented Scale', BuzzFeed, 17 September 2014, https://perma.cc/P37T-6CWW.
[368] Thomas Fox-Brewster, 'Is An American Company's Technology Helping Turkey Spy On Its Citizens?', Forbes, 25 October 2016, https://perma.cc/78HM-4D23.
[369] Bill Marczak et al., 'Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?' (Citizen Lab, 9 March 2018).
[370] BBC, 'How BAE Sold Cyber-Surveillance Tools to Arab States', *BBC News*, 15 June 2017, https://perma.cc/75ZM-NXYD.

innocuous link.[371] An IP address can be used to infer physical location, as IP addresses are often associated with geographical connection points, although this is unreliable: owner information is not always checked, the IP address can be easily spoofed, and multiple individuals can use the same connection point. This IP revealing software is widely available and not especially sophisticated. More importantly, those targeted were Twitter or Facebook users critical of the government, and, once their IP address was known, security forces in some cases raided the associated physical address and imprisoned those found. While this is not illegal under Bahraini law, which requires internet users to disclose subscriber information and has strict lese majeste clauses permitting imprisonment for insulting the head of state, NGOs argued that it contravenes international human rights of freedom of expression.

Three companies have been the focus of most reports associating targeted surveillance with human rights violations in Egypt and the Gulf states. The first of these companies is FinFisher, the example I used in the thesis introduction. Finfisher was formerly part of UK company Gamma International,[372] although it was based in Germany at the time of writing.[373] FinFisher offers several products including the targeted surveillance software "FinSpy". Documents obtained by Egyptian activists following the January 2011 revolution showed that the Egyptian internal security agency was invoiced by Gamma International for FinSpy installation in June 2010, although Gamma claimed no systems had been installed.[374] FinFisher technologies were also used in Bahrain against pro-democracy activists, lawyers and opposition leaders between 2010 and 2012.[375] Later, an investigation by Citizen Lab identified FinFisher products in Egypt, Oman, and Saudi Arabia (among many other states) in 2014 and 2015.[376]

---

[371] Bahrain Watch, 'The IP Spy Files: How Bahrain's Government Silences Anonymous Online Dissent', 1 August 2013, https://perma.cc/U4PX-JC6P.
[372] David Leigh, 'Offshore Company Directors' Links to Military and Intelligence Revealed', *The Guardian*, 28 November 2012, https://perma.cc/9MUT-9WWB.
[373] Finfisher, 'FinFisher - Excellence in IT Investigation', accessed 1 August 2017, http://www.finfisher.com/FinFisher/index.html.
[374] McVeigh, 'British Firm Offered Spying Software to Egyptian Regime – Documents'.
[375] Bahrain Watch, 'Bahrain Government Hacked Lawyers and Activists with UK Spyware', 7 August 2014, https://perma.cc/ZWV5-LCKB.
[376] Marczak et al., 'Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation'.

The second company is Hacking Team, an Italian company whose flagship product installs targeted surveillance software on a target device. Hacking Team provide both the software and the surrounding infrastructure (for example, the intermediate points between the target device and the customer's system through which the information is sent).[377] In 2012, this software was found on the device of a UAE dissident named Ahmed Mansoor,[378] who is a persistent critic of the UAE government on human rights issues and has been imprisoned and assaulted.[379] Their software was later identified by Citizen Lab in the UAE, Oman, Saudi Arabia, and Egypt.[380] In Saudi Arabia, this software was customised to install with a news app, 'Qatif Today'.[381] Qatif is a region in the east of Saudi Arabia with a predominantly Shia population and historically high levels of protest against discriminatory policies and excessive use of force by security agencies,[382] and this design suggests the scope of its intended targets. In Egypt, Hacking Team sent a contract for this software in January 2015 to the Technical Research Department (TRD),[383] a subsection of the Egyptian intelligence agencies who are associated more broadly with extensively catalogued human rights violations including torture and mistreatment as well as suppression of political opposition.[384]

The third company, NSO Group, is based in Israel and owned by a US investment group. It should be noted that the national identity of companies like NSO Group, given a large Israeli cybersecurity industry closely associated with the military, and Israel's 'outsider' status in the Wassenaar Arrangement, deserves closer attention than is permitted by the scope of this chapter. A Citizen Lab investigation (the Million Dollar Dissident report) indicated that intrusion software by NSO Group was used to obtain access to the phone of Ahmed Mansoor – who had earlier been

[377] Bill Marczak et al., 'Hacking Team's US Nexus' (Citizen Lab, 28 February 2014).
[378] Morgan Marquis-Boire, 'Backdoors Are Forever: Hacking Team and the Targeting of Dissent?' (Citizen Lab, 10 October 2012).
[379] Human Rights Watch, 'UAE: Investigate Attacks on Rights Defender', 3 October 2012, https://perma.cc/K7Q8-ZV3U.
[380] Bill Marczak et al., 'Mapping Hacking Team's "Untraceable" Spyware' (Citizen Lab, 17 February 2014).
[381] Morgan Marquis-Boire et al., 'Police Story: Hacking Team's Government Surveillance Malware' (Citizen Lab, June 2014).
[382] Toby Matthiesen, *The Other Saudis: Shiism, Dissent And Sectarianism* (New York, NY: Cambridge University Press, 2014).
[383] Privacy International, 'The President's Men?'
[384] Human Rights Watch, 'Egypt: Consolidating Repression Under Al-Sisi', 12 January 2017, https://perma.cc/65AH-JPF5.

targeted with FinFisher and Hacking Team software - in 2016.[385] NSO Group software is technically much more advanced than that of the other two companies, which reflects the increased sophistication of the capabilities available on the market. This relative sophistication in export-level technologies exists despite Israeli news reports suggesting NSO Group's most advanced capabilities were denied an export licence.[386]

In sum, this section has argued that from 2011 onwards, with an increased focus after the 2013 Snowden revelations, NGOs and media organisations reported extensively on the use of various types of filtering and surveillance software in Egypt and the Gulf states. Table 5 summarizes the presence of surveillance and filtering technologies in this region and identifies direct connections to human rights violations based on the reports above.

Table 5: Filtering and surveillance technologies and human rights violations

! = Direct association with HR violation		State						
		Bahrain	Egypt	Kuwait	Oman	Qatar	KSA	UAE
Technology	Targeted surveillance	HT! FF!	HT FF		HT FF	FF	HT FF	HT! NSO! FF!
	Filtering	NS BC	PR BC	NS BC		NS BC	SF BC	SF NS BC
	Mass surveillance	NSN!	NSN AM NR		EV	EV	EV	EV
HT=Hacking Team, FF=FinFisher, NSO=NSO Group, NS=Netsweeper, BC=Blue Coat, SF=Smartfilter, NSN= Nokia Siemens Networks, AM=Amesys, NR=Narus, EV=ETI Evident, PR=Procera/Sandvine								

6.2.2 Cybersecurity threats and human security

This section builds on the reports above to argue that NGOs aligned human rights values with dominant organisational conceptions of cybersecurity through the construction of targeted

[385] Bill Marczak and John Scott-Railton, 'The Million Dollar Dissident: NSO Group's IPhone Zero-Days Used against a UAE Human Rights Defender' (Citizen Lab, 24 August 2016).
[386] Times of Israel, 'Israeli Government Okayed Sale of Spyware That Exploits IPhones', 7 September 2016, https://perma.cc/62JF-CF2G.

surveillance companies as cybersecurity 'threat actors'. This alignment relied on discursive characteristics and technical concepts, as well as a deeper shift in the meaning of cybersecurity itself.

The initial overlap between surveillance and cybersecurity threats opened partly because media organisations sought comments on targeted surveillance from mainstream cybersecurity companies. For example, a report by UK left-wing newspaper The Guardian on the Finspy software included an interview with an employee of the cybersecurity company Trend Micro, who said that:

> Our position on commercial spyware is that if the monitoring is being done without the consent of the person being monitored then that would be the theft of information. There's certainly an ambiguity of selling that kind of technology to that type of regime. There are a lot of commercial tools to enable you to remotely monitor and manage computers but it's about how those tools are being used.[387]

By interviewing cybersecurity companies about Finspy, the Guardian implied that government targeted surveillance should be considered a cybersecurity threat. While this company, Trend Micro, commented to advertise their products – which they immediately amended to detect such software - the comment above is carefully worded. It emphasises the many different uses for surveillance tools (or 'remote monitoring') and remains vague about legitimate or illegitimate uses of those tools. Although it comes close to stating that human rights values are relevant due to the 'ambiguity' of working with 'that type of regime', this expert comment does not explicitly mention human rights *despite* the Guardian's implied association.

Other incidents involved an embrace of cybersecurity terminology to make the case that government surveillance is a cybersecurity threat to human rights. For example, the Bahrain Watch report on IP address location in the previous section involved technical analysis and victim cooperation resembling the post-incident investigations conducted by professional cybersecurity companies. Here, the mainstream cybersecurity terminology of phishing was used to describe the government's actions, adopting the technical language of cybersecurity to portray the government as a cybersecurity threat. Furthermore, some of the links did not just record the IP address, but also obtained credentials and downloaded probable spyware through apparently legitimate documents; these were referred to as 'malicious links' or 'malicious accounts'. The overarching frame of

[387] McVeigh, 'British Firm Offered Spying Software to Egyptian Regime – Documents'.

‘malicious actor’, from the dominant organisational conception of cybersecurity, was thus repurposed to highlight human rights violations, aligning the two sets of values in cybersecurity.

The clearest examples of alignment, however, occurred in relation to the three targeted surveillance companies in the previous section. The success of the portrayal of Hacking Team as a threat to individual rights was partly due to the creation of a series of cybersecurity-type reports on a ‘threat actor’, exactly in the manner of the cybersecurity companies examined in Chapter 5. Privacy International’s “The President’s Men?” report detailed the Hacking Team contract to Egypt, including ‘exposed’ pictures of the contract itself, while Citizen Lab released five consecutive reports - all with catchy titles and coordinated media coverage - focusing on the ‘malicious software’ used by Hacking Team. This series had all the hallmarks of the reports examined in the previous chapter, from codenames and campaign dates, with intelligence and political background and technical indicators. In doing so, Citizen Lab leveraged the genre established around threats to organisations and repurposed its discursive characteristics to highlight human rights violations.

The construction of NSO Group as a cybersecurity threat was also helped by the ‘Million Dollar Dissident’ report mentioned at the start of this chapter. It is instructive to examine the difference between this report and vague comments from cybersecurity company Trend Micro in the Guardian article quoted above, four years before the Million Dollar Dissident report. While in 2012 Trend Micro refused to explicitly characterise targeted surveillance software for government use as a threat to human rights, in 2016 another cybersecurity company, Lookout, not only stated this explicitly regarding NSO Group, but was involved in the investigation itself in tandem with Citizen Lab. This collaboration underlines the success of the alignment effort by NGOs, as human rights values became a central part of the cybersecurity landscape more broadly.

The alignment of human rights values with organisational cybersecurity discourses also led to the discovery of new human rights ‘threat actors’. Another 2016 Citizen Lab report identified “a campaign of targeted spyware attacks carried out by a sophisticated operator, which we call Stealth Falcon. The attacks have been conducted from 2012 until the present, against Emirati journalists,

activists, and dissidents."[388] Here the codename and campaign genre mentioned above was used not to recast an established surveillance supplier such as Hacking Team as a cybersecurity threat, but to create an entirely new threat actor solely around the protection of human rights values. This genre alignment also proved successful in several subsequent cases, including labelling phishing links sent to migrant workers in Qatar and Nepal as 'Operation Kingphish',[389] and similar links sent to human rights organisations in Egypt as 'Nile Phish'.[390] In each case, some association with government security forces or private contractors working on their behalf is implied if not explicitly stated.

It is important to note that although this alignment has so far only been considered in one direction – namely, aligning human rights values with organisational conceptions of cybersecurity - there are also some indications of alignment in the opposite direction. One example can be seen very early on in the development of cybersecurity threat intelligence, as Citizen Lab's Ghostnet report started the trend for cyber espionage reports in 2009.[391] Another is the coinage of "Bahamut" – in medieval Islamic mythology, a gigantic fish that supports the world - to describe phishing attempts against human rights activists across the Middle East. Although this was originally understood as a human rights issue, a later report on Bahamut by the same authors puts this threat actor into a standard cyber espionage frame, speculating that they might be contractors for a range of clients.[392]

To conclude this section, I place the alignment above in wider understandings of security drawing on both the NGOs themselves and critical security studies. The alignment of human rights values with organisational values in cybersecurity is similar to the expansion of the concept of security itself discussed extensively in the late 1990s and early 2000s under the label of 'human security'. The concept of human security aimed to destabilise established imaginaries of international security, and to replace such imaginaries with a more emancipatory security agenda based on human

[388] Bill Marczak and John Scott-Railton, 'Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents' (Citizen Lab, 29 May 2016).
[389] Amnesty International, 'Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal' (Amnesty International, 14 February 2017).
[390] John Scott-Railton et al., 'Nile Phish: Large Scale Phishing Campaign Targeting Egyptian Civil Society' (Citizen Lab, 2 February 2017).
[391] Citizen Lab, 'Tracking GhostNet: Investigating a Cyber Espionage Network' (Citizen Lab, 28 March 2009).
[392] Colin Anderson and Claudio Guarnieri, 'Bahamut, Pursuing a Cyber Espionage Actor in the Middle East' (Bellingcat, 12 June 2017), https://perma.cc/S8UW-45FU; Colin Anderson and Claudio Guarnieri, 'Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia' (Bellingcat, 27 October 2017), https://perma.cc/V57A-66MU.

rights.[393] This similarity is deliberate: the director of Citizen Lab, Ron Deibert, has explicitly stated that his aim is to promote an alternative 'human security' version of cybersecurity.[394]

However, Deibert sees his work as different to that of many civil society organisations operating in the same space. As he explained in a paper on the relationship between cybersecurity and civil society, in a passage worth quoting at length:

> For many who would characterise themselves as part of global civil society, "security" is seen as anathema. In today's world of exaggerated threats and self-serving hyperbole from the computer security industry, it is easy to dismiss security as a myth to be demolished, rather than engaged. Securitisation is associated with the defence industry, Pentagon strategists, and the cyber security military industrial complex. Many might question whether employing the language of security only plays into this complex and the growing might of cyberspace controls… As the securitisation of cyberspace builds momentum, it may be tempting for civic networks to either concede the terms of the security debate to the national security community, or resist it altogether.[395]

Deibert here portrays his civil society interlocutors as in a 'tempting' position of juxtaposing human rights values as an alternative to cybersecurity. He goes on to say that "that would be a mistake… What is urgently required now is the translation of that tradition [of liberal security] to the domain of cyberspace". In other words, *altering* rather than replacing cybersecurity.

Consequently, seeing the association of human rights values and surveillance technologies simply as the introduction of a new norm *within* cybersecurity is not quite accurate. While Deibert has been described by other scholars as a "left-leaning norm entrepreneur" in the manner of transnational advocacy networks, something more complex is going on.[396] The ability to redefine cybersecurity itself as focused on the protection of human rights values, just as human security redefines security discourses for human rights more broadly, depends not only on rethinking the concept of security but also on mirroring the micro practices, characteristics and genres of the dominant conception of cybersecurity. In other words, the less the association of human rights values

---

[393] Roland Paris, 'Human Security: Paradigm Shift or Hot Air?', *International Security* 26, no. 2 (1 October 2001): 87–102.
[394] Ronald J. Deibert, 'The Virtual Absence of Malice: Cyber Security and Threat Politics', *International Studies Review* 11, no. 2 (1 June 2009), p.374.
[395] Ronald J. Deibert, 'Towards a Cyber Security Strategy for Global Civil Society?' (Global Information Society Watch, 2011), pp.25-26.
[396] Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* 33, no. 1 (1 April 2012), p.163.

with surveillance technologies appears to be a new norm and the more it mirrors existing organisational values, the more successful it is. This is the moral manoeuvre of alignment.

Alignment is therefore a complement to norm studies, as new values are incorporated into cybersecurity by enlisting the dominant organisational values of cybersecurity in their support. Classic accounts of transnational advocacy networks, such as that of Keck and Sikkink, recognised this complexity when they acknowledged that the introduction of new norms depends on already available moral resources, but they do not specify how this dependency operates.[397] In contrast, this account emphasises how both the human rights and organisational values are reinterpreted by cybersecurity experts. In the last section of this chapter, I examine the relationship of this moral manoeuvre to a specific cyber norm: the 2013 amendment of the Wassenaar Arrangement on Dual Use Technologies.

6.3 The Wassenaar Arrangement

The Wassenaar Arrangement has been characterised as the first step towards the control of 'cyber weapons'.[398] Most accounts of the amendment of the Wassenaar Arrangement focus primarily on its role in restricting or changing the behaviour of the companies and states producing technologies captured by the amendment; in other words, how far it acts as a cyber norm. I investigate this aspect of the amendment in detail in Chapter 8, where I argue that the constraining power of the Wassenaar Arrangement is limited by the moral manoeuvre of manipulation.

In this section, I examine a different aspect of the amendment: its relationship to human rights conceptions of cybersecurity and the role of NGOs in defining the legitimacy of several standard cybersecurity professional practices. This section argues that the moral manoeuvre of alignment extends beyond the promotion of human rights values as part of cybersecurity, highlighting the wider debates into which NGOs were drawn. It first details the Wassenaar

[397] Keck and Sikkink, *Activists beyond Borders*, pp.34-35.
[398] Stevens, 'Cyberweapons', 10 January 2017.

Arrangement itself and its incorporation into US export policy, and then explores the questions of legitimacy that arose during this process.

6.3.1 US export policy

The NGO activities above formed the basis for international efforts to amend the Wassenaar Arrangement to control the export of surveillance technologies. The Wassenaar Arrangement is an arms control agreement implemented in 1996 and now including 41 state participants (not including Egypt and the Gulf states but including most of their primary arms exporters including the US and UK). The Wassenaar Arrangement controls not only arms exports, but also 'dual use technologies', defined to include use in human rights violations as well as more traditional security concerns. The Wassenaar Arrangement was amended in 2013 to include targeted surveillance technologies and some DPI-based surveillance technologies in the national export controls of its participating states.

Of course, many factors played a role in the amendment of the Wassenaar Arrangement.[399] These include the initial proposal by the UK and France and the advocacy efforts of Marietje Schaatke in the European Parliament, while concurrent negotiations regarding the 2014 Arms Trade Treaty may have been a factor in the swift adoption of the amendment by EU states. Nonetheless, the NGO and media reports in the previous section, especially those on Egypt and the GCC, were crucial, as they were used by advocates of the amendment to provide the only public examples of an association between surveillance and human rights violations. The resulting export controls were largely based on the technical details provided in these reports. The US played a central role in the debate over the amendment, as many vocal advocates and critics were based there or contributed to US-based publications. In this section, I focus on the Wassenaar Arrangement from a US perspective. I will examine the reaction by other surveillance suppliers and exporting states in Chapter 8.

Responsibility for regulation of US exports is split between the State Department, which controls items under the Arms Export Control Act through the US Munitions List (UML), and the

[399] These factors are considered more generally in Jennifer Erickson, *Dangerous Trade: Arms Exports, Human Rights, and International Reputation* (New York: Columbia University Press, 2015), p.35.

Department of Commerce, which controls items under the Export Administration Act through the Commerce Control List (CCL) and the Export Administration Regulations (EAR).[400] The Wassenaar Arrangement dual use list is incorporated into the CCL and administered by the Bureau of Industry and Security (BIS) within the Department of Commerce, although other departments (including Defense and Energy) are involved in the decision process. Exports include 'deemed exports', defined as the release of controlled technology to foreign persons in the US.

There are specific human rights criteria under the broad heading of 'foreign policy' controls (other headings are national security and short supply).[401] Because these controls are classified as foreign policy, there is no stipulation that they cannot be outweighed by national security considerations. More specifically, items which may be used for internal repression are classified as 'crime control' items, which includes reasons of anti-terrorism and regional stability. Crime control items are considered unilaterally, meaning that while BIS "considers international norms regarding human rights and the practices of other countries that control exports… these controls may differ from controls imposed by other countries" and it must also judge that "any adverse effect on the economy of the United States does not exceed the benefit to US foreign policy objectives".[402] The relevant foreign policy objective is "to promote the observance of human rights throughout the world", based largely on State Department reports on human rights, which include a section on internet freedoms. These decisions are "considered favourably [i.e. licence granted] on a case-by-case basis …. Unless there is evidence that the government of the importing country may have violated internationally recognised human rights".[403] A 2014 report from BIS clarifies that these controls are "intended to deter the development of a consistent pattern of human rights abuses" and "distance the US from such abuses".[404]

[400] This and the following paragraph draw heavily on Tim Maurer, Edin Omanovic, and Ben Wagner, 'Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age' (New America Foundation, Open Technology Institute, Digitale Gesellschaft, Privacy International, March 2014).
[401] Maurer, Omanovic, and Wagner., p.7.
[402] Maurer, Omanovic, and Wagner., p.9.
[403] Maurer, Omanovic, and Wagner., p.9
[404] Bureau of Industry and Security (USA), '2014 Report on Foreign Policy Based Export Controls' (US Department of Commerce, 2014).

In the US, there was also a specific historical precedent that significantly affected the implementation of the Wassenaar amendment. The amendment was discussed against a backdrop of disagreements over the export of cryptography between privacy advocates and the technical community on one hand, and the US government on the other, now known as 'the crypto wars'.[405] Until 1996, cryptography had been classified as a munition under US export regulations, due to its predominant use in military and government devices. Following three landmark cases which challenged this classification – one concerning the posting of encryption technology to a website, where it could be downloaded by foreign persons[406] - under the Clinton administration export regulations were loosened and a range of exemptions were granted for commercial use of encryption, including a general software exemption for mass market products,[407] which enabled the growth of internet commerce in the early 2000s.[408] However, this debate polarised both sides, and the introduction of new Wassenaar additions was seen through this polarised frame as an attempt to stifle the internet industry and free enterprise.

The Wassenaar amendment controls elements of both targeted and mass surveillance technologies.[409] With regards to mass surveillance technologies, the filtering technologies associated with human rights violations in the previous section and the underlying DPI technology itself are excluded from the control because they do not have a 'mapping' capability to link devices and individuals together. With regards to targeted surveillance technologies (known as 'intrusion' technologies in the Wassenaar language), it is only the surrounding systems, not the means of intrusion itself, that are controlled (the delivery mechanism, not the warhead, to use Wassenaar's missile analogy).

---

[405] Steven Levy, *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age* (Penguin, 2001).
[406] Ronald Stay, 'Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann', *Georgia State University Law Review* 13, no. 2 (1996).
[407] Ira Rubinstein and Michael Hintze, 'Export Controls on Encryption Software', in *Coping With US Export Controls 2000* (Practising Laws Institute, 2000).
[408] Danielle Kehl, Andi Wilson, and Kevin Bankston, 'Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s' (New America Foundation, Open Technology Institute, June 2015).
[409] Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies'.

The amendment succeeded despite significant resistance in the US both before and after its implementation, with ongoing contest and amendments to the amendment up to the time of writing.[410] This resistance came from both politicians and expert testimonies arguing that a wide range of cybersecurity technologies are functionally identical to those controlled by the amendment. Consequently, they held that the separation of both targeted and mass surveillance technologies from certain cybersecurity technologies in the way attempted by the Wassenaar Arrangement is impossible.[411] This certainly does not apply to all cybersecurity technologies (most have no 'dual use' possibilities whatsoever), but there is a substantial grey area, to which I will return below.

The Wassenaar amendment initially accommodated these concerns by including a 'mass market' exemption, putting outside the domain of the control any technologies that are readily available without customisation or specific customer relationships. However, BIS excluded cybersecurity items from their exemption for mass market software.[412] The rationale was that this matches their historic encryption controls originally debated in the crypto wars. Because much cybersecurity software includes encryption, one may otherwise encounter a situation where it is controlled under one description, and not under another.[413]

A second issue complicating US implementation of the Wassenaar amendment was that BIS had a policy of "presumptive denial for zero-day exploits and rootkits".[414] Both are technical terms for elements often present in intrusion software: zero-day exploits use vulnerabilities not known to the manufacturer of the product at the time of production,[415] and rootkits control the most basic processes of a device, making them more powerful and harder to detect. Like the Wassenaar

[410] Shaun Waterman, 'The Wassenaar Arrangement's Latest Language Is Making Security Researchers Very Happy', Cyberscoop, 20 December 2017, https://perma.cc/V7PH-KJ4X; Garrett Hinck, 'Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research', Lawfare, 5 January 2018, https://perma.cc/5NHM-L4FL; Penny Pritzker, 'Response to Letter Regarding Implementation of the Wassenaar Arrangement "intrusion Software" and Surveillance Technology Provisions' (US Department of Commerce, 1 March 2016), https://perma.cc/9ABQ-6567.

[411] US House of Representatives Subcommittee on Information Technology, 'Transcript of Discussion "Wassenaar: Cybersecurity and Export Controls"', 12 January 2016, pp.8-9.

[412] Access et al., 'Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements', 20 July 2015.

[413] Bureau of Industry and Security (USA), 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items', *Federal Register* 80, no. 97 (20 May 2015): 28853–63.

[414] Bureau of Industry and Security (USA).

[415] Allen Householder, 'Like Nailing Jelly to the Wall: Difficulties in Defining "Zero-Day Exploit"', Software Engineering Institute, Carnegie Mellon University, 7 July 2015, https://perma.cc/VQ5Y-3JMY.

Amendment, this policy controls not the exploits themselves but the technologies within which they are embedded.[416] This policy is controversial because the US government also participates in the zero-day market to improve its own offensive capabilities.[417] The US government thus gains as much by *restricting* potential exports as by encouraging them, because it can retain powerful exploits for its own use.[418]

Throughout the debates over the introduction and implementation of the Wassenaar amendment, the political and epistemic weight against it and the highly technical character of the distinctions and concepts used, meant that the same NGOs that produced the reports in the previous section became expert commentators on the issues as well as advocates and supporters. For example, a widely used document summarising the Wassenaar amendment evaluated the advantages and disadvantages of the amendment in an unmistakably professional tone:

> Clearly defined and well enforced Intrusion Software and IP Network Surveillance controls can lay the groundwork for a constructive and expansive role for export controls in the promotion of human rights and cyber security goals. As export control authorities consider license applications and industry education, it is incumbent to ensure that these new regulations are narrowly applied to control equipment, software, and technologies that are substantially designed for surveillance.[419]

BIS proposed a new rule including intrusion and surveillance software in their controlled exports list in May 2015,[420] and took the unusual step of soliciting public comments prior to implementation, partly due to the controversies above. As a counterweight to industry resistance against the Wassenaar amendment, NGOs focused on fine distinctions and technological arguments for the practicality of the amendment, presenting themselves not as purely advocacy groups but also as expert commentators and cybersecurity professionals. A submission of comments to the U.S. Department of Commerce from several bodies including the Electronic Frontier Foundation, Human

---

[416] Bureau of Industry and Security (USA), 'FAQs: Intrusion and Surveillance Items', US Department of Commerce, accessed 2 August 2017, https://perma.cc/6TRT-HM3Y.
[417] Mailyn Fidler, 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, Summer 2015), https://papers.ssrn.com/abstract=2706199.
[418] Sam Jones, 'Leaked CIA Cyber Tricks May Make Us WannaCry Some More', Financial Times, 25 May 2017, https://perma.cc/CJT6-HEP7.
[419] Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', p.6.
[420] Bureau of Industry and Security (USA), 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items'.

Rights Watch and the Open Technology Institute, with individuals all involved in creating the reports in the previous section, illustrates this nicely. In this submission they explicitly claimed a technical rather than advocacy purpose, despite their familiarity with the latter:

> The goal of our comments is both to provide specific information about aspects of the rule that are either ambiguous or otherwise concerning, and to offer concrete recommendations to address these problems.[421]

This document highlights how the NGOs above played a crucial role in discussions over the Wassenaar Arrangement and its implementation in the US by combining detailed technical claims and normative motivations. This section builds on the view of norm studies that treaties, laws and agreements into international politics are dependent on the work of transnational advocacy networks, and their focus on expertise as a key factor in this process. I now show how the moral manoeuvres framework can extend this analysis further by exploring the concepts of legitimacy and dual use.

6.3.2 Legitimacy and dual use

The concept of dual-use played a key role in the amendment of the Wassenaar Arrangement. Exploring this concept helps us to understand how NGOs aligned cybersecurity with human security. Specifically, I argue that the concept of dual use shifted from being a choice between a security-oriented or threatening use on one hand and a benign or peaceful use on the other, to become a much finer distinction between legitimate and illegitimate technologies *within a single security space*, namely, cybersecurity. NGOs engaged on both sides, contributing to the definition of legitimate cybersecurity technologies as well as 'illegitimate' ones associated with human rights violations.

The Wassenaar Arrangement initially defined dual-use as goods and technologies that could be used to produce weapons (i.e. items on the controlled Munition List of the Arrangement) even though that was not their sole function. In the words of the Arrangement: "dual-use goods and technologies to be controlled are those which are major or key elements for the indigenous

[421] Access et al., 'Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements', p.4.

development, production, use or enhancement of military capabilities."[422] Understandably, although the definition of a security-relevant use was precisely defined through inclusion on the Munition List, the potential non-security uses were not defined, and vary substantially in different cases.

There is a concept of dual-use for digital technologies that follows this conception between security-relevant and non-security uses. Much of the malicious software in the incidents reviewed in Chapter 5 are not only 'hacking' tools but also have 'legitimate' uses, such as the disk driver which overwrites data in Shamoon. This disk driver could be used by IT professionals to reformat hard drives, a necessary and routine task outside the security domain. There are thus many benign uses *outside cybersecurity* for the technologies described as cybersecurity threats.

This sense of dual use can also be employed for surveillance technologies. Although the definition of a cybersecurity threat for surveillance technologies is based on human rights rather than the protection of organisations, filtering and surveillance technologies also have many non-security uses. For example, DPI-based surveillance not only enables governments to collect data on target populations, but also enables network administrators to perform traffic management and quality of service tasks unrelated to any conception of cybersecurity. Similarly, filtering devices can prevent employees accessing social media sites, increasing productivity rather than security, while targeted surveillance software uses remote control mechanisms similar to those used by many apps to troubleshoot and obtain advertising data with little consent from the device owner. This sense of dual-use for digital technologies mirrors the original Wassenaar Arrangement meaning, and is one of the reasons it was considered a suitable mechanism to control such technologies.

However, there is a second, more complex, sense of dual-use that distinguishes between two different types of security-relevant uses: on one hand, uses by 'threat actors' (whether organisational or rights-based), and on the other, benign uses *to combat security threats.* This is a reinterpretation of dual-use as between legitimate and illegitimate security technologies, rather than security-relevant and non-security technologies.

[422] Wassenaar Arrangement Secretariat, 'Criteria for the Selection of Dual-Use Items' (Adopted in 1994 and amended by the Plenary in 2004 and 2005, 2005), https://perma.cc/U5MZ-3JG7.

Two examples were used most often by cybersecurity professionals in arguing against the Wassenaar amendment. First, they argued that surveillance is a common cybersecurity practice. This could be large-scale surveillance, for example at the internet gateway of a large organisation, or targeted surveillance of specific devices to detect malicious software on those devices ('endpoint protection'). Another common cybersecurity practice, the automated detection of cybersecurity threats based on anomalous behaviour in networks, depends on rules and 'signatures' (malware characteristics) functioning within DPI-based monitoring systems. Some of the surveillance and filtering systems analysed in the second section of this chapter explicitly advertise cybersecurity services as part of their product capability: both Smartfilter and Netsweeper block malicious software based on signatures as well as prohibited websites. Because the surveillance systems used by governments are commercial, they have legitimate security uses that can differ only from illegitimate ones in terms of the target itself or the specific rule written by the customer.[423]

The second example commonly used in this debate was the practice of 'penetration testing', which involves compromising a client's network *exactly* as a hacker would, but with an agreement to do so from the client. This is the basis for an entire industry of 'vulnerability disclosure' and 'bug bounty' programs, where independent researchers test popular products for vulnerabilities using a range of hacking techniques. In an extreme reading of this practice, it implies that there can be no difference between legitimate and illegitimate cybersecurity technologies, as in that case penetration testing would be impossible. The question is merely one of intention and scale: how far the hacker or vulnerability researcher actually completes the compromise rather than providing proof of concept (a distinction over which bug bounty programmes argue at length).

The problem is that both technological and social factors must be used to identify legitimate and illegitimate uses. Both examples above have interlinked social and technological elements, as they are established practices in the cybersecurity community not due only to technological necessity, but also a range of political and economic drivers shaping the industry. Of course, the necessity of including social and technological factors in determining dual-use is not unique to

[423] Hinck, 'Wassenaar Export Controls on Surveillance Tools'.

cybersecurity, and the Wassenaar Arrangement has established mechanisms for doing so. Both the mass market exemption and the indirect control of targeted surveillance technologies in the amendment were designed to avoid controlling the cybersecurity practices above. Furthermore, the amendments to the amendment itself agreed by the US in 2017 followed existing arms control practice by including a socially defined condition of 'end-use decontrol' – e.g. to share vulnerabilities for the purposes of research or to counter cybersecurity incidents.[424]

The key point is that the debate between advocates and critics of the Wassenaar amendment was not over whether human rights violations occurred, nor over whether such violations could be associated with surveillance and filtering technologies. Both the human rights NGOs and the cybersecurity industry *largely took this for granted*. Instead, the argument was about whether such violations were an unfortunate but unavoidable by-product of a legitimate cybersecurity practice or represented the foundation of a new rights-based conception of cybersecurity. Crucially, the alignment of human rights values with the prevalent values of the cybersecurity industry documented in the second section of this chapter meant that the legitimate cybersecurity aim itself could not be seriously challenged by NGOs. Instead, the debate centred on the importance of ensuring that that aim was not adversely affected by the Wassenaar amendment, pushing NGOs to argue as experts about the uses of technologies that were *not* associated with human rights violations.

Norm-based accounts of NGO activity could easily miss this aspect of the Wassenaar amendment. In contrast, a moral manoeuvres approach focuses on the wider value structure at work in cybersecurity, highlighting how actors such as NGOs reinterpret a range of values in conjunction with technical claims to achieve their normative aims. The moral manoeuvres approach also emphasises how actors attempt to redefine the issue area itself: here, NGOs put forward a version of human cybersecurity aligned with the dominant organisational version. Others disagreed: for example, the Wassenaar amendment itself called its mass market exemption a 'cybersecurity exemption', suggesting that cybersecurity was everything outside these tools. I will return to the

[424] Waterman, 'The Wassenaar Arrangement's Latest Language Is Making Security Researchers Very Happy'.

Wassenaar Arrangement in Chapter 8, examining how its amendment fits into the separate moral manoeuvre of manipulation performed by surveillance suppliers and exporting states.

***

This chapter has examined cybersecurity experts outside Egypt and the Gulf states, although these states featured heavily in the investigations that aligned human rights values with organisational values in cybersecurity. The chapter focused on cybersecurity experts worldwide and policy debates in the US, because the expert community in the region did not generally acknowledge human rights framings of cybersecurity. However, this chapter has deliberately not interrogated the context in which these surveillance and filtering technologies were implemented: namely, how was cybersecurity understood in Egypt and the Gulf states by the governments *themselves*? In the next chapter, I examine government organisations in cybersecurity.

Chapter 7: Appropriation

Raʾif Badawi, the creator of the "Free Saudi Liberals" website, was arrested by the Saudi authorities on 17 June 2012. He had run the website since 2006 and had been detained and questioned about its content in 2008. A month before his arrest, he used it to declare a celebratory day for Saudi liberals. Badawi was charged under the 2007 cybercrime law – among others[425] - for posts made by him and others on this website.[426] He was sentenced to 10 years in prison and 1000 lashes; the first 50 were carried out in January 2015, but after international protests the remainder were deferred on health grounds. While recognising the severity of the human rights violations in this incident, this chapter focuses on a slightly different question: is Raʾif Badawi a cybercriminal?

Behind this question is the appropriation of cybersecurity, including key terms such as cybercrime, by specific government departments in Egypt and the GCC states in order to suppress political opposition. This chapter details the second of four moral manoeuvres in cybersecurity in Egypt and the GCC states. Appropriation inverts the moral manoeuvre of alignment, constructing human rights activists and political dissidents as a cybersecurity threat to governments, rather than the other way around. Appropriation is performed by governments – specifically ministries of interior and security agencies – invested in an expansive definition of national security.

The alternative explanation of this phenomenon in norm studies is as state adoption or resistance to an emerging cybersecurity 'norm' of the Budapest Convention on Cybercrime. However, such an explanation does not adequately capture the way state organisations view the Budapest Convention as only one resource among many in creating cybercrime laws. A norm-based approach also does not explain how state organisations redefine the concept of cybercrime while also appearing to endorse freedom of expression internationally. The conscious engagement in

[425] Other charges included apostasy and insulting his father. It is unclear from public reports in both English and Arabic what combination of charges led to the specific sentence imposed, although the apostasy charge is the most severe; it allows capital punishment and was advocated by some Saudi conservatives.
[426] BBC, 'Saudi Arabian Blogger "Flogged"', *BBC News*, 9 January 2015, https://perma.cc/36JH-YJUS; BBC, 'Saudis Uphold Blogger's 1,000 Lashes', *BBC News*, 7 June 2015, https://perma.cc/5RJK-P5MF; ʿAbdallah Al-Barqawi, 'Tanfiz Hukm Al-Jild ʿala Raʾif Badawi Bisubbub ʿibarat Kufriyya Wa ʿuquq Walidihi [Sentence of Lashes Imposed against Raif Badawi for Expressions of Unbelief and Insulting His Father]', Sabq, 9 January 2015, https://perma.cc/Q99Y-5F39.

cybersecurity strategies with those of international partners, and the recognition that compromise is necessary on both sides, means these governments cannot simply be seen as resisting relevant norms.

This chapter has three sections. The first section shows how national cybersecurity strategies disguise appropriation by perpetuating the ambiguous organisational conception of cybersecurity outlined in Chapter 5. The second section examines the appropriation of the concept of cybercrime through the Budapest Convention on Cybercrime and the Arab Convention on Combatting Information Technology Offences, as well as cybercrime laws adopted by all seven states in draft or final form. The third section argues that appropriation is also *institutional*, stemming from domestic struggles between interior ministries, security services, telecommunications agencies and IT departments.

7.1 Cybersecurity strategies

This section argues that multiple clusters of values are referenced in national cybersecurity strategies in Egypt and the Gulf states, but they are deliberately kept abstract and ambiguous. This abstraction is a crucial part of my argument, as it disguises the moral manoeuvre of appropriation detailed later in this chapter.

To put cybersecurity strategies in context, 'national strategies' are themselves a peculiar text in this region. National cybersecurity strategies for the Gulf states follow broader state policy. All GCC states have long-term national plans – the most well-known being Saudi Arabia's bold 'Vision 2030", championed by the Crown Prince Muhammad bin Salman – and these display three broad similarities. First, they claim to refocus the economy from extractive industries towards technology and innovation, whether through smart cities, e-government, or other skilled sectors such as health and finance. Second, they aim to reduce the role of the public sector in all areas of life. Third, they aim to reduce high expatriate numbers through extensive training and preferential treatment for citizens. Egypt has also had many strategic plans both internally and delivered by development consultants. National cybersecurity strategies echo these wider characteristics, presenting an image of carefully planned cybersecurity governance to their audiences.

In this region, national cybersecurity strategies are written for a predominantly international audience. Having a strategy is a requirement of many cybersecurity maturity models, such as the ITU cyber readiness index, and international bodies collect and compare cybersecurity strategies from around the world.[427] These strategies are often written by international consultants in English and translated into Arabic. The language of these strategies is hyperbolic, vague, and full of jargon: for example, the Qatari strategy claims that "this is an integrated and holistic approach that will enhance synergies, avoid duplication, and maximize resource utilisation in managing the dynamic environment and emerging threats in cyberspace."[428] Such language is easy to ignore, or at least to dismiss as mere marketing, with no significant role in cybersecurity more broadly. I argue instead that it is a key part of the moral manoeuvre of appropriation, disguising the alteration of values and technical claims.

The sources are not quite as simple as the phrase 'national strategies' might suggest, given the lack of availability of many government documents in this region. There is only one national cybersecurity strategy named as such that has been published in a final form in Egypt and the Gulf states, in English or Arabic (that of Qatar). Instead, I used publicly available documents that are as close to the national cybersecurity strategies as possible. The sources for this analysis are listed in Table 6.

[427] https://ccdcoe.org/cyber-security-strategy-documents.html
[428] ictQatar, 'Qatar National Cyber Security Strategy' (Government of Qatar, May 2014), p.vii.

Table 6: Documents used to analyse national cybersecurity strategies

State	Document	Available	Secondary sources
Egypt	National ICT strategy 2012-2017 (2012)	Yes	New Egyptian constitution (2014)
UAE	National Cybersecurity Strategy (NCS) (2014)	No	Presentation at RSA conference on the strategy (2015), Dubai NCS (2017)
Saudi Arabia	National Information Security Strategy (NISS) (2013)	No	Draft NISS (2011), National Cybersecurity Centre profile (2017)
Qatar	National Cybersecurity Strategy (2014)	Yes	N/A
Oman	High Level Cybersecurity Strategy and Master Plan (2013)	No	E.Oman strategy (2010), ITA cybersecurity mission and goals (2018)
Kuwait	National Cybersecurity Strategy (2017)	No	Announcement and summary of NCS (2017)
Bahrain	National Cybersecurity Strategy (2017)	No	NCS summary on TRA website (2017), e.Gov strategy (2016)

The object of cybersecurity in these strategies is described variously as cyber, digital, information or electronic security (in Arabic: *al-ʾamn al-sibrani*, *al-ʾamn al-raqmi*, *ʾamn al-muʿalumat* or *al-ʾamn al- al-ʾiliktruni* respectively). In other contexts, scholars have argued that this linguistic difference captures important differences in national approach; for example, the societal concerns included in Russian or Chinese concepts of 'information security' rather than 'cybersecurity'.[429] However, this is too simplistic a conclusion for situations where there are many terms in play at the same time. The focus of this chapter is thus on the alteration of specific clusters of values and technical claims, not whether such a shift can be captured in a binary distinction between the term 'cyber' on one hand and 'electronic' or 'information' on the other. Translation is a crucial aspect of moral manoeuvres, but it is more subtle than often supposed.

[429] Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English', in *2013 5th International Conference on Cyber Conflict*, ed. K Podins, J Stinissen, and M Maybaum (Tallinn: NATO CCDCOE, 2013).

The Egyptian constitution of 2014 is perhaps the clearest example of a translation capturing political differences, as Article 31 states that "the security of information space (*fidaʾ al-muʿalumat*) is an integral part of the system of national economy and security. The state commits to taking the necessary measures to preserve it in the manner organised by law."[430] Given the wide powers allocated to military and security agencies under this constitution, and the censorship practiced by these organisations under President Al-Sisi, the 'preservation' of 'information space' appears to clearly take the side of the cyber sovereignty position in global debates over internet governance. However, as the strategies below demonstrate, the hybrid position of Egypt and the Gulf states discussed in Chapter 3 complicates this binary reading.

National cybersecurity strategies often include only an abstract summary of the issue. For example, the Bahrain strategy claims to "establish a secure cyber-space (*fidaʾ al-ʾiliktruni ʾamin*) to safeguard national interests and protect the Kingdom of Bahrain against cyber-threats (*tahdidat al-ʾamn al-ʾiliktruni*) to reduce risks."[431] In Dubai, this is phrased even more broadly: "The goal is to build a more secure information society that is perfectly aware of cyber security risks (*makhatir al-ʾamn al-ʾiliktruni*). One of the key objectives of this strategy is to address any risks, threats or attacks."[432] In Saudi Arabia, the strategy aims to build "an effective and secure national information security environment (*biaʾat ʾamn al-muʿalumat*)",[433] while the NCSC claims to "build a resilient and secure cyberspace that protects national and citizens' interests".[434]

Given this abstract tone, the term 'malicious actor' – a key part of the ambiguous professional discourse examined in Chapter 5 - is the most prominent characterisation of cybersecurity threats in these strategies. For example, the Dubai strategy states that "An open and free cyber space provides value… It is important to protect this value against the risks of malicious

[430] The Arab Republic of Egypt, 'Egypt's Constitution of 2014' (Constituteproject.org, translated by International IDEA, 2014).
[431] Government of Bahrain, 'Kingdom of Bahrain - EGovernment Portal Cybersecurity Strategy', eGovernment Portal, 3 October 2017, https://perma.cc/RSL4-FPJA (ENG), https://perma.cc/NNP2-CGBJ (AR).
[432] Government of Dubai, 'Dubai Cyber Security Strategy' (Dubai Electronic Security Center, 2017).
[433] MCIT (Saudi Arabia), 'National Information Security Strategy' (Ministry of Communications and Information Technology, January 2011).
[434] National Cyber Security Center, 'Profile - Introducing the National Cyber Security Center' (Governnment of Saudi Arabia, 2017).

activities and disruptions… Dubai is a major target for malicious actors".[435] Qatar also claims that it is "an attractive target for malicious actors who seek to cause disruption and destruction".[436] It is worth noting that the adjective 'malicious' has several translations. In sentence from the Dubai strategy above, the phrase 'malicious actors' is replaced by electronic attacks (*al-hujumat al-ʾiliktruniyya*), while the Qatar strategy uses 'biased sides' (*jihat mughrida*) in the sentence above and elsewhere 'malicious/evil intentions' (*nawaya khabitha*) for insider threats.[437] The latter echoes a similar description for malicious software (*barmajiyyat khabitha*). The term 'malicious' thus performs a similar role in incorporating a range of organisational values into a single ambiguous term in both English and Arabic.

Even when these strategies provide a more detailed breakdowns of cybersecurity threats, these descriptions retain ambiguous organisational conception of cybersecurity. For example, Bahrain states that "Malicious actors – hackers, organised criminals and possible foreign governments can exploit this gap [in security]. Thus, a comprehensive national strategy is required to address current and rising cyber-threats as well as reduce risks."[438] Qatar lists the main threats as "hacktivists, Advanced Persistent Threats, Cyber Crime Syndicates, and Malicious Insiders".[439] Saudi Arabia summarises cybersecurity threats as "cyber-terrorism, cyber-war, and cyber-espionage", and highlights the overlap between different threats noted in Chapter 5: "Every day Gulf Cooperation Council businesses are targeted by nation-state actors for cyber exploitation and theft…. Many of the same vulnerabilities used to steal intellectual property can also be used to attack the critical infrastructures."[440] The abstract and generalised tone of these strategies therefore perpetuates the ambiguities of the organisational conception of cybersecurity identified in Chapter 5.

These strategies also endorse human rights values, especially individual freedom and privacy, in an equally abstract style. For example, the objectives of Saudi Arabia's strategy aims to "enable information to be used and shared freely and securely", while the National Cyber Security

[435] Government of Dubai, 'Dubai Cyber Security Strategy', p.9.
[436] ictQatar, 'Qatar National Cyber Security Strategy', p.3.
[437] ictQatar, p.4.
[438] Government of Bahrain, 'Kingdom of Bahrain - EGovernment Portal Cybersecurity Strategy'.
[439] ictQatar, 'Qatar National Cyber Security Strategy', p.4.
[440] MCIT (Saudi Arabia), 'National Information Security Strategy', pp.2,81.

Centre seeks "to realize a safe, open and stable information society".[441] The Dubai strategy desires "a free and secure cyber world", claiming that "cyber space needs to remain open to innovation and free flow of ideas, information, and expression", although "due consideration should be made to maintain the proper balance between open technology and the individual rights of privacy."[442] The Qatar strategy claims that their "values in cybersecurity" are to "show tolerance and respect", and embrace "the free flow of ideas and information".[443] In Bahrain, the aim is to "maintain the rights and values of individuals."[444] This language echoes wider contests over human rights values noted in Chapter 3, where alternative institutions are set up to mimic the language of genuine human rights bodies.

However, even in the rarefied world of cybersecurity strategies this endorsement of human rights values is qualified by vague references to safety and care. The Saudi strategy emphasises the cultural and economic threats of information to the state, a point not made by senior Saudi figures writing in US journals.[445] In Kuwait, "the strategy is primarily intended to promote the culture of cybersecurity which supports the safe and right use of the electronic space",[446] while Qatar aims to "foster a culture of cyber security that promotes safe and appropriate use of cyberspace".[447] The Dubai strategy states that "cyber space attacks lead to a variety of threats, such as: fraud, espionage, terrorism, violation of privacy, and defamation."[448] "Careful use of social media" is therefore a "baseline control" that "should be established, maintained and supported by Dubai individuals in their implementation", along with system updates, firewalls, and password management.[449] The phrase 'careful use' is ambiguous between care in clicking on links and sharing potentially infected documents on the one hand, and self-policing of content on the other.

---

[441] MCIT (Saudi Arabia); National Cyber Security Center, 'Profile - Introducing the National Cyber Security Center', pp.iv,12.
[442] Government of Dubai, 'Dubai Cyber Security Strategy', pp.7,13.
[443] ictQatar, 'Qatar National Cyber Security Strategy', p.17.
[444] Government of Bahrain, 'Kingdom of Bahrain - EGovernment Portal Cybersecurity Strategy'.
[445] Naef bin Ahmed Al-Saud, 'A Saudi Outlook for Cybersecurity Strategies: Extrapolated from Western Experience', *Joint Forces Quarterly*, no. 64 (2012): 75–81.
[446] Staff Report, 'CAIT Chief Briefs HH the Amir on National Cybersecurity Strategy - Vision to Protect Kuwait's National Interest', Arab Times, 31 July 2017, https://perma.cc/KTQ7-GW8G.
[447] ictQatar, 'Qatar National Cyber Security Strategy', p.v.
[448] Government of Dubai, 'Dubai Cyber Security Strategy', p.12.
[449] Government of Dubai, p.25.

Egypt's ICT strategy demonstrates this abstract and ambiguous tone clearly, partly because of Egypt's larger international role in the debate over internet governance examined in Chapter 3, but also due to its publication date in 2012, shortly after the revolution and before the constraints on the public sphere and higher security imperatives initiated by President Al-Sisi from 2013. It was then relaunched under Al-Sisi as a 2014-2017 rather than 2012-2017 strategy, but no other changes were made.[450] On one hand, it states that "Telecommunications Law No. 10 of 2003, for example, contains certain articles that require amendment in line with Egypt's democratic transition that will promote political openness and protect freedom of expression."[451] On the other hand, it also includes the qualification of these values noted above, claiming to "bring about the desired balance between the considerations of freedom as a fundamental human right and privacy considerations and national security".[452] Consequently, "the availability of information [that] could harm national security of Egypt or the exposure of relations with other countries at risk under the banner of freedom is not acceptable."[453] Here the national strategy incorporates a separate cluster of values under an expansive definition of national security, as well as an abstract endorsement of human rights values.

Finally, these national strategies also display a contradictory orientation to international cyber norms, most relevantly the Budapest Convention on Cybercrime (treated in detail later in this chapter). The Budapest Convention is only referenced in the Omani and Egyptian strategies. In Oman, the Budapest Convention is described as one source among many for its cybercrime law:

> As the Omani society nowadays witnesses an enormous revolution in information technology, it was necessary to set a law that protects networks and devices from illegal hacking attempts… The issuance of the Cyber-Crimes Law was based on the Budapest Convention as well as local, regional and international legislations.[454]

This statement portrays the Budapest Convention as a genuine influence in the way norm theories would expect, although, as explored below, not to the extent that Oman acceded to the Convention.

---

[450] MCIT (Egypt), 'Publications - Egypt's ICT Strategy 2014 -2017', Ministry of Communications and Information Technology, 2014, https://perma.cc/X6G3-WT3F.
[451] MCIT (Egypt), 'National ICT Strategy 2012-2017: Towards a Digital Society and Knowledge-Based Economy' (MCIT, 2012), p.9.
[452] MCIT (Egypt), p.33.
[453] MCIT (Egypt), p.33.
[454] Government of Oman, 'Information Security - Omanuna Portal', Omanuna, 26 March 2018, https://perma.cc/8VYS-5KSW.

However, in Egypt the situation is less clear. In the English version of the strategy, the draft cybercrime law is explicitly claimed to originate from both international and domestic sources, including:

> International Telecommunication Union (ITU) recommendations regarding cybersecurity; relevant Indian law; the Legislation Management Draft Law of the Ministry of Justice; the Decision Support Center Draft Law; the Convention on Cybercrime (Budapest Agreement) of the Council of Europe; and "Cybercrime," by information security expert Ahmed El-Sobky.[455]

Again, the Budapest Convention is presented as an influence on national cybersecurity strategy in a similar manner to Oman. However, the Arabic version of the strategy strangely omits this paragraph. The most plausible interpretation of this omission is that the English strategy aims to communicate internationally that it is based on a range of sources including the Budapest Convention, whereas this is not a relevant consideration for an Arabic-speaking audience. If correct, this reading suggests that the Budapest Convention is merely utilised by governments to signify agreement with *international* audiences, rather than being a genuine influence on their national strategy and regulation (and thus present also in the Arabic version).

The Saudi Arabian strategy contains a similar contradiction between domestic and international stances. After claiming that Saudi Arabia is "quickly aligning itself with international standards and capabilities to detect and respond to cybercrime", the strategy states:

> The NISS makes an important distinction between internal cybercrime laws and procedures and the requirements necessary when dealing with these issues at the international level. In order to effectively operate on the international cybercrime stage, the Kingdom may need to forego a rigid interpretation of its own legal standards and procedures and adopt a more flexible legal approach to work cooperatively with international partners.[456]

It explains that this is because "domestic and international, as well as legal and cultural challenges arise when dealing with cybercrime and the interpretation of legal standards, procedures and law. Specifically, Sharia law is "applied to some forms of cybercrime", which "on the international stage,

[455] MCIT (Egypt), 'National ICT Strategy 2012-2017: Towards a Digital Society and Knowledge-Based Economy', p.35.
[456] MCIT (Saudi Arabia), 'National Information Security Strategy', p.65.

will be more difficult".[457] These quotations reveal a fascinating dissonance between the internationally accepted and domestically appropriated versions of cybercrime, even in public government documents. As in Egypt, the Saudi Arabian strategy suggests that international agreements such as the Budapest Convention have very limited influence on domestic cybercrime law. It also acknowledges that there are substantial differences in the concept of cybercrime between domestic and international levels. The abstract tone and internationally oriented language of national cybersecurity strategies disguises these differences, which are the subject of the following section.

7.2 Cybercrime laws

Cybercrime laws were drafted between 2006 and 2016 throughout Egypt and the Gulf states. In this section I argue that these laws consisted of an expansion of the scope of 'cybercrime' from economic concerns such as fraud and espionage to also include political speech online. This is the moral manoeuvre of appropriation: the reinterpretation of values and technical concepts for a specific goal. This section is based on the texts of the laws themselves, in English and Arabic, as well as prior analysis of the laws by policy and human rights organisations. My analysis of the use of these laws is based on interviews and investigation, including systemic searches of news articles and human rights reports.

I first stress that 'cybercrime' is an English term with no agreed equivalent in Arabic. While many professional documents in Arabic use the loan word *sibrani* (cybercrimes would thus be *al-jaraʾim al-sibraniyya*), this neologism is not used in legal terminology. Instead, the legal Arabic equivalents are electronic crimes (*al-jaraʾim al-ʾiliktruniyya*), information crimes (*jaraʾim al-muʿalumat*), or information technology crimes (*jaraʾim tiqniyyat al-muʿalumat*). The English translation of these terms, for example in unofficial English-language versions of these laws created by law firms or in the English-language version of local newspapers, is nearly always 'cybercrime'.

[457] MCIT (Saudi Arabia), p.66.

7.2.1 Texts

This section argues that the development of cybercrime laws in Egypt and the Gulf states is not captured by norm-based explanations of either localisation of or resistance to an international norm represented by the Budapest Convention on Cybercrime. Instead, the concept of moral manoeuvres provides a better explanation of the emergence of these laws as it shows how, despite not acceding to the Budapest Convention, these states use it as one resource among many for their own aims, rather than a source of normative pressure to which they must respond.

The main international norm regarding cybercrime is the Budapest Convention on Cybercrime agreed by the Council of Europe in 2001. None of the states considered in this thesis have acceded to the Budapest Convention (accession is available to non-members of the Council of Europe, while signature is only available to members). At the time of writing, there were 64 ratifications or signatures/accessions to the Convention, only two of which are in the Middle East (Tunisia and Israel).[458] On the face of it, Egypt and the Gulf states cannot 'localise' this norm, in Acharya's terms, as they are not 'norm-takers': they have not accepted it as an international norm in the first place.[459] An alternative reading of Egypt and the Gulf states in relation to the Budapest Convention, then, would be as resisting the emerging norm represented in the Budapest Convention by not acceding to the Convention. However, this is also not quite accurate, as the Budapest Convention *does* play a role in cybercrime in Egypt and the Gulf states at both national and regional levels, but as only one resource among many. I first consider the only regional agreement on cybercrime and then investigate then domestic laws themselves.

Both the UN and the ITU have been involved in the creation of regional cybercrime regulation. An interviewee with extensive experience of the UN Economic and Social Commission for Western Asia (ESCWA) described its role as follows:

[458] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime' (European Treaty Series - No.185, 15 August 2018), https://perma.cc/7NQM-U764.
[459] Acharya, 'How Ideas Spread', p.240.

> At ESCWA we try to complement ITU, not necessarily deliberately handling things separately but it could be by accident. We made a project of cyber legislation, drafting a cyber law – we were not doing the technology but the law. ITU were also starting cybersecurity issues, focusing on standards and technology, and we use their data (I-32).

The result of these efforts by both ESCWA and the ITU is the only international agreement in the region on cybersecurity: The Convention on Combating Information Technology Offences (*jaraʾim tiqniyyat al-muʿalumat*) by the Arab League. This convention was initially signed in December 2010, and it has been ratified by Egypt and all GCC states other than Saudi Arabia.

Many articles of the Arab Convention that define cybercrime are drafted broadly. For example, Article 12 includes "The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that disturbs modesty through information technology".[460] This includes much artistic work or content that could offend certain segments of the population. Article 15 – "offences related to terrorism" – includes a clause criminalising "attacking religions or beliefs", and another on the "dissemination and advocacy of the ideas and principles of terrorist groups".[461] As 'terrorism' itself is widely defined in Egypt and the GCC states, this article enables the criminalisation of almost any political writings online. Finally, Article 21 states that "Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology". Overall, the Arab Convention expands the definition of cybercrime to focus on various kinds of online content, especially political speech. This is an expansion of rather than a shift away from an economic concept of cybercrimes, as the Convention also includes articles on copyright infringement, fraud, and electronic payment.

The Arab Convention inverts the rights-based conception of cybersecurity considered in the previous chapter. This can be seen by comparing its article on privacy - Article 14 criminalising "offences against privacy by means of information technology" – to an analysis by Muhammad Al-Taher, writing for an Egyptian human rights group in 2015. Using the version of the Egyptian

[460] Al-Jamiʿat Al-Dawl Al-ʿArabiyya [The Arab League], 'Al-Itifaqiyya Al-ʿarabiyya Limukafahat Jaraʾim Tiqniyyat Almuʿalumat [the Arab Convention on Combatting Information Technology Crimes]' (Al-Jamiʿat Al-Dawl Al-ʿArabiyya [The Arab League], 21 December 2010).
[461] League of Arab States, 'Arab Convention on Combating Information Technology Offences' (League of Arab States General Secretariat, 21 December 2010).

constitution updated in the mid-1990s as a comparison, rather than the new constitution passed in January 2014, Al-Taher argued that the Arab Convention posed a threat to freedom of expression and individual privacy, stressing the lack of protection against privacy both domestically and through sharing information between countries. He also highlighted the vagueness of Article 14 itself, which leaves open the bearer of the right of privacy and could equally be used to prevent individuals criticising governments and leaders as much as preventing access to individuals' data.[462]

The Arab Convention is different in several key ways to the earlier Budapest Convention. Hakmeh highlights the similarities between the two, claiming that "provisions [of the Arab Convention] are in fact *almost* the same as those of the Budapest Convention, especially in relation to procedural powers and international cooperation" (my italics).[463] However, the key word here is 'almost', as none of the articles that include political and socially controversial content in the Arab Convention above (12, 14, 15 or 21) are in the Budapest Convention. Rather than representing resistance to the Budapest Convention, the Arab Convention is thus a mixture of direct influence from the earlier text and additions that repurpose the Budapest Convention towards political speech.

The only other regional agreement relevant to cybercrime legislation is a 2012 GCC joint security agreement mentioned in Chapter 3. Although this agreement does not explicitly address cybersecurity or cybercrime, it covers related matters such as information-sharing between governments. The third clause of the agreement states that states will "take legal measures in what is considered a crime according to their laws when its citizens or those living on its territories interfere in the internal affairs of other countries."[464] This agreement allows expanded definitions of cybercrime to be applied across state boundaries. Online commentary on events in other countries

[462] Muhammad Al-Tahir, 'Taʿliq ʿala Al-Itifaqiyya Al-ʿarabiyya Limukafahat Jaraʾim Tiqniyyat Almuʿalumat [Comments on the Arab Convention for Combatting Information Technology Crimes]' (Muʾassasat Huriyyat Al-Fikr Wa Al-Taʿbir [Foundation for the freedom of thought and expression], 12 March 2015), https://perma.cc/DUB8-6END.
[463] Joyce Hakmeh, 'Cybercrime and the Digital Economy in the GCC Countries' (Chatham House - The Royal Institute for International Affairs, June 2017), p.11.
[464] Toumi, 'GCC Ministers Sign Major Security Agreement'; Gulf Cooperation Council, 'Security Agreement Between Countries of the Gulf Cooperation Council' (GCC, 13 November 2012), https://perma.cc/3W3J-RTYM.

can thus be defined as cybercrime, allowing states to coordinate the suppression of political opposition.

The Arab Spring and near contemporaneous signing of the Arab Convention was the catalyst for the spread of cybercrime laws in the GCC. Between 2011 and 2017, Saudi Arabia, Oman, and the UAE all updated earlier laws while Bahrain, Qatar and Kuwait implemented new laws (Table 7).

Table 7: Cybercrime laws in Egypt and the GCC

State	Electronic transactions law	Cybercrime law
Oman	2008	Penal code amended with chapter on computer crime 2001, Cyber Crime Law 2011
UAE	2002	Law No. 2 of 2006, Law No. 5 of 2012 Concerning Combating Information Technology Crimes
Saudi Arabia	2007	Anti-Cyber Crime Law 2007, updated 2015
Qatar	2010	Cybercrime Prevention Law 2014
Bahrain	2002	Law No. 60 of 2014 Concerning Information Technology Crimes
Kuwait	2014	Law No.63 of 2015 Concerning Combating Information Technology Crimes
Egypt	2004	Laws 2015 and 2016 Concerning Electronic Crimes discussed by Parliament, approved 2018

Like the Arab Convention, these cybercrime laws also expand the concept of cybercrime to cover political speech online. Hakmeh argues that all GCC countries other than Bahrain have "additional offences not foreseen in other legal instruments" in their cybercrime laws.[465] In her words, "most GCC cybercrime laws have been subject to heavy criticism by human rights organisations for limiting free speech and imposing self-censorship on citizens and activists".[466] Duffy's 2014 analysis supports this view, arguing that all six states characterise defamation or libel

[465] A 2018 update focusing on their human rights implications was published too late to be included in this thesis. Hakmeh shared an early draft with me, and its conclusions mirror those reached in this section.
[466] Hakmeh, p.9.

as a criminal offence without permitting truth as a defence.[467] This legal environment privileges government actions; for example, in the UAE the libel of a public servant is an aggravating factor rather than a higher bar for prosecution due to public interest defences. Like Hakmeh, Duffy emphasises that these laws put forward wide definitions of 'public morals' and 'national unity', which means that many social media comments, including any political opposition, could be considered a cybercrime.

Crucially, these laws go beyond the alternative norm-based explanation of localisation, as they actively exploit the ambiguities within abstract concepts of cybercrime rather than responding to international normative pressure. For example, the cybercrime law in Saudi Arabia was updated in 2015 with what was termed a 'naming and shaming' clause for offenders, allowing a name and details of their offence to be published in local newspapers with the costs to be paid by the person convicted.[468] Similarly, the updated Omani law in 2011 has a section explicitly titled "content crimes", covering any use of ICTs to "produce or publish or distribute or purchase or possess whatever might prejudice the public order or religious values."[469] The updated UAE law in 2012 is one of the starkest examples of cybercrime extending to political opposition as well as economic concerns. As well as the national unity clause quoted in the thesis introduction, Article 9 prevents almost any form of online political debate:

> Shall be punished by temporary imprisonment and a fine not in excess of one million dirhams whoever publishes information, news, statements or rumors on a website or any computer network or information technology means with intent to make sarcasm or damage the reputation, prestige or stature of the State or any of its institutions or its president, vice-president, any of the rulers of the Emirates, their crown princes, or the deputy rulers of the Emirates, the State flag, the national peace, its logo, national anthem or any of its symbols.[470]

[467] Matt Duffy, 'Arab Media Regulations: Identifying Restraints on Freedom of the Press in the Laws of Six Arabian Peninsula Countries', *Berkeley Journal of Middle Eastern & Islamic Law* 6, no. 1 (1 April 2014), p.1.
[468] Staff Report, 'Al-Shura Al-Saʿudi Yudifu ʿaqubat Al-Tashhir ʾila Nizam Mukafahat Al-Jaraʾim Al-Muʿalumatiyya [Saudi Council Adds Naming and Shaming Punishment to the Cybercrime Law]', Al-Sharq Al-ʾAwsat, 18 March 2015, https://perma.cc/4QXP-Y8JR.
[469] Government of Oman, 'Royal Decree No 12/2011 Issuing the Cyber Crime Law' (Government of Oman, 2011).
[470] Government of the UAE, 'Federal Decree-Law No. (5) of 2012 On Combating Cybercrimes'.

Another good example is the Kuwait cybercrime law, which was signed in 2015 and included very similar provisions to those detailed above. Interestingly, this law had been considered even before the Arab Spring: a leaked US cable in 2010 quoted Minister of the Interior Sheikh Jabar Al-Khalid Al-Sabah as complaining that "politics was hindering progress on… many other important bills, including one to criminalize cyber crimes".[471] However, human rights organisations argued that the Kuwait law was "an effective barrier to critical political speech over the Internet"[472] and "a direct assault on the right to freedom of opinion and belief and the right to freedom of expression".[473] The expansion of cybercrime in these laws is thus far more than localisation or even translation of an existing norm: it is the active alteration and renegotiation of a cluster of values around national security, along with technical terms like 'cybercrime'. This is the phenomenon I seek to capture using the concept of moral manoeuvres.

Finally, Egypt's cybercrime law has followed a more contentious path than its equivalents in the Gulf states. A draft cybercrime law was first mentioned in a government-wide ICT strategy in 2012. In a similar manner to those in the Gulf states, this draft law doubled the penalties for those committing "information crimes" (*jaraʾim al-muʿalumat*) with the intent to damage public interest or an individual public authority.[474] At least three further drafts have been proposed since the June 2013 coup, in April 2015, May 2016 and June 2018.[475] The latest draft was approved by parliament in June 2018 although it had not passed into law at the time of writing.[476]

[471] Wikileaks, 'US Embassy Kuwait City - Kuwait Interior Minister Sounds Alarm on Iran; Offers Assurances on GITMO Returnees and Security' (Wikileaks Public Library of US Diplomacy, 17 February 2010), Public Library of US Diplomacy, https://perma.cc/A79J-WF2E.
[472] Human Rights Watch, 'Kuwait: Cybercrime Law a Blow to Free Speech', Human Rights Watch, 22 July 2015, https://perma.cc/265U-VVAB.
[473] Reporters without Borders, 'New Cyber Crimes Law Restricts Free Expression and Targets Online Activists', 21 January 2016, https://perma.cc/M9ZB-6VRH.
[474] MCIT (Egypt), 'National ICT Strategy 2012-2017: Towards a Digital Society and Knowledge-Based Economy', p.35.
[475] Muhammad Yusif, 'Al-Watan Tanshuru Nus Qanun Al-Jarimat Alʾiliktruniyya ʾamam Al-Nuwab [Al Watan Publishes the Text of the Electronic Crimes Law before Parliament]', Al-Watan, 11 May 2016, https://perma.cc/KAX8-SUQH; Khalid Negm, 'Draft Law Concerning Electronic Crimes' (Leaked draft available on Scribd, April 2015), https://perma.cc/H4BS-VLGQ.
[476] ʿAbd Al-Basir Hassan, 'Majlis Al-Nuwab Al-Misri Yaqirru Qanun Mukafahat Al-Jarimat Al-ʾiliktruniyya [Egyptian Parliament Decides on Cybercrime Law]', BBC News, 7 June 2018, https://perma.cc/5DWF-Y64S. It is not included in the analysis here, although its provisions appear similar.

The proponent of the 2015 draft, Minister for Communications and Information Technology Khalid Negm, claimed that it was in part prompted by the Arab Convention.[477] The 2016 draft then increased the severity of the first in a similar way to the updated cybercrime laws in the GCC states, increasing the punishments for vaguely defined crimes of harming national unity and public morals.[478] According to privacy advocates in Egypt, in the first version "punishments are harsher when an individual is found to have committed a crime against the state or a corporation".[479] One commentator noted that the 2016 draft also included concepts such as 'illegitimate ideas', which were not present in the first version.[480] This repeats the pattern of broad terminology and expansive definitions in the Gulf states.

Other differences between the 2015 and 2016 drafts point to the coalitions and compromises necessary for cybercrime legislation in a large and diverse state such as Egypt. Both versions block "any words or figures, pictures or movies, or any propaganda material that threatens national security". However, the second version (article 14) does not have the provision for doing this in advance of permission by the criminal court (article 19 in the first draft), instead specifying only that the court will respond within the day of the blocking request. This is an admittedly thin safeguard on unilateral action introduced into the draft at a time when the Egyptian courts were under increasing pressure from the Al-Sisi government to support an expansive definition of national security.

So far, I have shown that the texts of the laws themselves form part of the moral manoeuvre of appropriation, as they expand the definition of cybercrime to include political opposition while also addressing economic threats. This is the stage at which Duffy and Hakmeh conclude their analyses, as it is not possible to ascertain from a purely textual analysis whether political speech or economic threats are the primary target of this legislation. To answer this question, I turn to interviews and reports on the use of these laws.

---

[477] Ragab Saad, 'Egypt's Draft Cybercrime Law Undermines Freedom of Expression', Atlantic Council, 24 April 2015, https://perma.cc/9ATE-HNNA.
[478] Mohamed Abdelaal, 'Egypt's New Cybercrime Law: Another Legislative Failure', Jurist, 9 July 2016, https://perma.cc/HED5-X2G7.
[479] Tom Rollins, 'Egypt's Cyber Crime Bill', Mada Masr, 24 May 2015, https://perma.cc/A2NM-CB9L.
[480] Mohamed Hamama, 'Egypt's New Cybercrime Bill Could Send You to Prison', Mada Masr, 12 October 2016, https://perma.cc/9QGR-SUFD.

7.2.2 Use

The purpose of the cybercrime laws above was summarised well by the interviewee with experience of UN ESCWA quoted at the start of the previous section. When I asked this interviewee about the purpose of cybercrime laws, they replied:

> At the national level, there is the threat of social media, as they are frightened by what can take place on social media, it can affect national sovereignty from the inside not the outside. Please make this anonymous, as it is controversial. This pushed the adoption of the cybercrime laws, protecting people inside from cybercrimes but also punishing them. There are lots of taboos in the region related to religion and/or politics. It is seen as a threat. (I-32).

This response indicates that the primary purpose of cybercrime legislation in the region is to suppress political opposition rather than prevent economic threats. This interviewee also emphasised the sensitivity of the subject, indicating that this purpose is hidden beneath the abstract strategies considered in the first section of this chapter. When I asked the interviewee what they thought about the human rights issues raised by cybercrime laws, their reply was revealing:

> This is not in line with our mandates. ESCWA is a social and economic department, while UNESCO would do ethics. We are all technicians and engineers and the issue of ethics is a bit different from our area of expertise. We don't want to step on UNESCO (I-32).

This response deserves a close reading. It wholeheartedly adopts the early technocratic approach to cybersecurity governance noted in Chapter 3. However, the interviewee also acknowledges that ESCWA's technocratic approach cannot be justified on the same grounds as that of the ITU, as it does not have the technical knowledge to implement technical standards. Instead, although cybercrime laws *are* within ESCWA's remit, their moral dimensions are downplayed. This evasion of responsibility is justified through a hyper-awareness of other departments: 'we don't want to step on UNESCO'. Far from exerting international pressure on Egypt and the Gulf states to conform to a norm on cybercrime, this interviewee suggests that some international actors do the opposite, skirting controversial aspects of international conventions precisely to avoid enforcing a particular norm or rule of behaviour. Technical expertise is enlisted to facilitate this avoidance.

This characterisation of international organisations has one exception. In all the conference documents I collected, human rights issues around cybercrime were only mentioned by one cybersecurity professional: Muhammad Al-Guindy, president of a professional cybersecurity association in Egypt and regular contributor to the Cybersecurity for Energy and Utilities conference series, as well as a member of the ITU. His 2012 study of cybercrime legislation in the region argued that "most governments in the region are violating the privacy of citizens and don't pay attention to even basic human rights that will be challenging when drafting cyber legislation".[481] Similarly, in a 2014 conference 'threat report', Al-Guindy, like other professionals, argued that "cyber regulations are poor in Middle East and even lack the correct definition of cybercrime", because "due to the political issues, most cyber laws are drafted to suppress freedom of speech and do not address the real threat of cybercrime".[482]

It is thus worth exploring Al-Guindy's position in more detail, and I do so using conversations with an interviewee familiar with his work. This interviewee claimed that, despite the surface appearance of the conference discourse, "cybersecurity experts in the region understand the importance of human rights when it comes to cyber legislation" (I-56). This interviewee then said:

> Culture and history play very important role in shaping how people think, specially policymakers. When it comes to cyber laws or cybercrime legislation, it is no difference. They look at it from their traditional point of view which is how to limit, block or censor specific tools or technology not to accept and regulate the technology (I-56).

This interviewee places the appropriation of the concept of cybercrime within the longer history of censorship and a restricted public sphere considered in Chapter 3. They then went on to explain the position of governments with regard to cybersecurity professionals in this appropriation:

> Even if they cooperate with local technical expertise, they will have the hidden political agenda... Political issues are always the driving force of drafting such laws, not the need to prevent attacks or crimes. Political issues including but not limited to democracy, freedom of speech and human rights (I-56).

[481] Mohamed N. El-Guindy and Faisal Hegazy, 'Cybercrime Legislation in the Middle East: The Road Not Travelled' (Information Systems Security Association (ISSA), 27 February 2012), https://perma.cc/T5JL-8K45.
[482] Mohamed N. El-Guindy, 'Middle East Cyber Security Threat Report 2014' (Cybersecurity for Energy and Utilities, 25 December 2013), https://perma.cc/HB2A-DUZL.

This interviewee suggests that even when cybersecurity professionals are involved in the drafting of laws or national strategies there is always a 'hidden political agenda'. This agenda is at its core 'political issues', meaning political speech online and opposition to the government, rather than cyber 'attacks or crimes'. Furthermore, for this interviewee, cybersecurity professionals participate in this appropriation even though they 'understand the importance of human rights'. This provides a different perspective on the lack of engagement with human rights values in the regional professional community considered in the previous chapter, suggesting that this avoidance is strategically motivated in order to maintain their position as expert advisors.

Other interviewees agreed that cybercrime laws in Egypt and the Gulf states were designed to suppress political opposition. An expatriate working alongside government security agencies in the Gulf remarked that "the police only really care about social media, because that's what affects the nationals" (I-7). The implication is that the police were not motivated to investigate cybercrime as it would be characterised in his own (European) jurisdiction – i.e. as a primarily economic problem - and instead focus on domestic political struggles.

One surprising comment came from a UAE national at NESA, the UAE cybersecurity agency. He was nonplussed when I asked him about cybercrime legislation, saying that "the cybercrime laws do not really come across my radar, that's more about using social media to harm the UAE government, and we are concerned more with national security" (I-26). While the laws themselves offer an expansive definition of national security, and are promoted as a key step in cybersecurity, their irrelevance to the work of people in NESA is striking, suggesting that the shift to suppress political opposition in these laws is so comprehensive that they are not considered important by those dealing with other types of cybersecurity threat.

One of the benefits of analysing cybercrime legislation in terms of moral manoeuvres compared to that of norms is that it highlights how international agreements are resources used strategically by actors for their own ends – in this case suppressing political opposition - rather than sources of normative pressure which are merely adjusted to suit local requirements. The strategic use of the Budapest Convention is illustrated by a Qatari government interviewee, who said that:

> Everyone references the Budapest Convention, but crime has changed. We need to look at our cybercrime legislation, and ask are they a deterrent or are they obsolete? Do you need cybercrime laws? Or do we need more privacy? (I-4).

The Budapest Convention here is not a norm in the sense of a clear standard of behaviour (and Qatar did not accede to it in any case). Instead, it is something that can be 'referenced', but only once the domestic goals of cybercrime legislation have been decided. Another interviewee working with the Qatari government summarised the contradictions created by such references, saying that: "if you put this – cyber monitoring - into cybersecurity then everything becomes cybersecurity. These are very different problems. People do use cybersecurity with different meanings in mind" (I-36).

As the interviews above suggest, these cybercrime laws have all been used to target political speech online, highlighting how appropriation is driven by actors invested in an expansive definition of national security. I now detail these uses in each state in turn.

In the UAE, the cybercrime law was used in 2013 to charge the son of one of 94 defendants associated with Al-Islah, a political group accused by the UAE government of affiliation with the Muslim Brotherhood, after he published details about their trial.[483] Al-Islah was then designated a terrorist group by the UAE in 2014. A prominent political dissident, Nasser bin Ghaith, was charged under the cybercrime law in 2016 after he criticised the UAE and Egyptian government. In this case, the cybercrime law was used to criminalise his claims of mistreatment in an earlier trial as the posting of information "intended to damage the UAE".[484] Ahmed Mansoor, the dissident considered in the introduction to the previous chapter, was also tried under cybercrime laws.[485] Finally, the extension to political opposition also applies to non-nationals; in 2016 an Omani was jailed for three years after criticising the UAE's conduct in the war in Yemen in a Whatsapp audio recording.[486] After the Qatar

[483] Human Rights Watch, 'UAE: Unfair Mass Trial of 94 Dissidents', Human Rights Watch, 3 April 2013, https://perma.cc/43WC-NSG2.
[484] Human Rights Watch, 'UAE: Free Two Jailed for Criticizing Egypt', Human Rights Watch, 15 May 2016, https://perma.cc/JJX2-RNGR.
[485] Staff Report, 'UAE Rights Activist Ahmed Mansoor Put on Trial in Abu Dhabi', Al-Jazeera, 18 April 2018, https://perma.cc/8MWW-JCMV.
[486] Staff Report, 'Omani Jailed for Insulting UAE on Whatsapp', Al-ʿArabi Al-Jadid, 29 February 2016, https://perma.cc/2ULR-LTFQ.

crisis in June 2017, the UAE attorney general stated that showing sympathy for Qatar online would be treated as a cybercrime, resulting in prison sentences between three and fifteen years.[487]

In Saudi Arabia, the cybercrime law was also used regularly to prosecute political opposition. As detailed in the introduction to this chapter, the liberal dissident Raʾif Badawi was sentenced under the cybercrime law in 2013.[488] A year later, the head of a human rights organisation in Saudi Arabia was also sentenced to seven years' imprisonment under the cybercrime law.[489] In 2015, a lawyer who had represented Raʾif Badawi and who founded the rights organisation Saudi Monitor for Human Rights was sentenced to fifteen years including cybercrime charges.[490] Other lawyers confirmed the use of the cybercrime law to prosecute the 'spreading of rumours' over Twitter in 2017.[491]

In Oman, the cybercrime law was used to charge an individual who interviewed striking oil workers in 2012 and made other political statements online, although he was then convicted of insulting the Sultan rather than under the cybercrime law.[492] In 2015, a government critic was sentenced to three years in prison for critical blog posts under the cybercrime law.[493] The editor of a politically independent newspaper in Oman, Al-Zaman, was charged under the cybercrime law after an article that criticised the judiciary in 2016.[494] The newspaper was shut down a year later.

In Bahrain, the most consistent use of the cybercrime law was against Nabeel Rajab, a prominent political activist, who led demonstrations in the 2011 protests and has been given prison sentences multiple times for his opposition to the government. According to his own testimony, he

[487] Thamer Al Subaihi, 'Supporting Qatar on Social Media a Cybercrime, Says UAE Attorney General', The National, 7 June 2017, https://perma.cc/K7Y2-8ST5.
[488] Human Rights Watch, 'Saudi Arabia: Free Editor Held Under Cybercrime Law', Human Rights Watch, 16 July 2012, https://perma.cc/3EEJ-XYXJ.
[489] Reporters without Borders, 'Cyber Crime Law Used Again to Silence Dissident Voices', 1 July 2014, https://perma.cc/2M9U-S5E2.
[490] Human Rights Watch, 'Saudi Arabia: 15-Year Sentence for Prominent Activist', Human Rights Watch, 7 July 2014, https://perma.cc/8QNA-8U4K.
[491] ʿAbdallah Al-Barqawi, 'Mutalabat Bimuʿaqaba Murawaji Shaʾiʿat "Al-Qurarat" ʿabr Muwaqiʿa Al-Tawassul [Demands to Punish the Promotion of "Low" Rumours on Social Media]', Sabq, 18 November 2017, https://perma.cc/5K8R-SV5G.
[492] Human Rights Watch, 'Oman: Rights Routinely Trampled', Human Rights Watch, 18 December 2014, https://perma.cc/66TQ-TDS6.
[493] Human Rights Watch, 'Oman: 3-Year Sentence for Rights Activist', Human Rights Watch, 23 March 2015, https://perma.cc/A49P-2FJD.
[494] Human Rights Watch, 'Oman: Journalists Arrested for Criticizing Judiciary', Human Rights Watch, 5 August 2016, https://perma.cc/FX3Y-6RBR.

was arrested and interviewed in 2015 and 2016 by the Cyber Crimes department following anti-government tweets, and remained in prison at the time of writing.[495] His charges included "insulting a neighbouring country" in relation to Saudi Arabia.[496]

In the other GCC states, Kuwait's cybercrime law was used in 2016 to charge a blogger who criticised the emir.[497] The structured searches used for this section identified no instances of Qatar's cybercrime law being used to suppress political opposition. However, human rights organisations highlight the potential for the cybercrime law to violate freedom of expression through the example of a poet sentenced to fifteen years in prison in 2013 for indirectly criticising the ruling family.[498] This poet, Muhammad Rashid Al-Ajami, was pardoned in 2016.

Across the GCC, these cybercrime laws are used in conjunction with other legal structures. In a survey of laws preventing freedom of expression in the Arab world, Ben Hassine argues that the precise combination of legal instruments differs considerably from state to state. The only Gulf state she examines in detail is Saudi Arabia, where she argues that anti-terror laws are the main tool used by the state to suppress political opposition.[499] As seen in the example of Raʾif Badawi, blasphemy, social order, and cybercrime laws are often used as a combination of offences for the same act.

Egypt is absent from the above analysis, as it has only a draft cybercrime law and consequently no cybercrime prosecutions. However, as Ben Hassine argues, Egypt already uses a variety of anti-terror and anti-protest laws to control online political activity. The anti-protest laws are especially successful in this aim, as encouraging or inciting people to protest online is a more serious offence in these laws than taking part in the protest itself. This focus on protests as a conduit for political opposition reflects Egypt's experience of the January revolution in 2011. It also highlights the violent responses of security forces to later protests, including the massacre of at least

[495] Nabeel Rajab, 'Letter From a Bahraini Jail', *The New York Times*, 4 September 2016, https://perma.cc/HH4R-6WZP.
[496] Bahrain Center for Human Rights, 'Updates: Arrest and Detention of BCHR's President Nabeel Rajab', Bahrain Center for Human Rights, 8 August 2017, https://perma.cc/39UJ-KBFH.
[497] FIDH, 'Kuwaiti Cyber Crimes Law Silences Dissent: Ongoing Prosecution of Sara Al-Drees', Worldwide Movement for Human Rights, 12 December 2016, https://perma.cc/YR93-Q4B8.
[498] Amnesty International, 'Qatar: New Cybercrimes Law Endangers Freedom of Expression', Amnesty International, 18 September 2014, https://perma.cc/4ZBS-732Q.
[499] Wafa Ben Hassine, 'The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online' (Electronic Frontier Foundation, April 2016).

700 people at Rabiʿa Square in 2013, and the regular disappearance and torture of activists and protesters since.[500]

In sum, this section has demonstrated that the governments of Egypt and the Gulf states appropriated the concept of cybercrime to counter political opposition. This tactic was combined with a similarly broad definition of other key legal terms such as terrorism, and strict anti-protest and media laws. Together, these laws incorporate a cluster of values under an expansive definition of national security. The data presented here is better explained by the moral manoeuvre of appropriation than as norm resistance or localisation, as these states actively reinterpret organisational conceptions of cybersecurity and use the Budapest Convention only as one resource among many to do so. However, this section has largely treated the state as a cohesive entity. In the next section, I examine internal struggles *between* state organisations that are an essential part of this moral manoeuvre.

7.3 Cybersecurity organisations

This section argues that between 2011 and 2017 there was a shift in cybersecurity responsibility from telecoms and IT ministries to ministries of interior and security agencies, marking an institutional as well as conceptual appropriation of cybersecurity.

The first cybersecurity action of many governments, including Egypt and the Gulf states, is to create a national computer emergency response team (CERT).[501] Even if these are little more than a public-facing website and contact details, these organisations enable the receipt of technical cybersecurity alerts and participation in organisations such as FIRST, a non-profit international grouping of public and private CERTs. Due to their technical functions, CERTs initially sit within the IT or telecoms regulator or telecoms ministry. However, this initial ownership is often challenged by other government departments. As one interviewee remarked, "one of the problems is the lack of agreed government frameworks for ownership. Ministry of defence? Ministry of interior? Often it

[500] Orla Guerin, 'The Shadow over Egypt', BBC News, 23 February 2018, https://perma.cc/B5UW-PZKE.
[501] Also known as CSIRTs

shouldn't be in either" (I-39). Another stressed that "there is a - let's call it - 'healthy' level of competition between government departments, either they are not conscious, or they think others can't deliver" (I-41). This competition is especially fierce because sensitive technologies such as signals intelligence (SIGINT) are the main sources of data about cybersecurity threats. As an interviewee explained, generalising across the Gulf states:

> SIGINT was run by sensitive units within ministries (blackboxed even from the rest of the ministry). But cyber was run by IT teams. The former didn't want their capability interfered with. But the latter thought 'we need to bring these things together' (I-49).

Consequently, there are several departments in most states with a significant responsibility for cybersecurity. Table 8 provides an overview of these institutions in Egypt and the GCC states and the year of creation.

Table 8: Cybersecurity institutions in Egypt and the GCC

Institution	Egypt	UAE	Saudi Arabia	Qatar	Oman	Kuwait	Bahrain
Ministry	MCIT (1999)	n/a	MCIT (2003)	MCIT (2003)	MTC (2001)	CAIT (2006)	CIO (2002)
Regulator	NTRA (2003)	TRA (2003)	CITC (2003)	ictQATAR (2004)	TRA (2002) ITA (2006)	CITRA (2014)	TRA (2002)
CERT	egCERT (2009)	aeCERT (2006)	CERT.sa (2006)	QCERT (2006)	OCERT (2010)	n/a	CERT.bh (2014)
Cybersecurity organisation	HCCS (2014)	NESA (2013)	NESC (2013) CSC (2017)	*Role fulfilled by CERT*	*Role fulfilled by CERT*	*Role fulfilled by CITRA*	*Role fulfilled by CIO*
Cybersecurity strategy	National ICT Strategy (2012)	NCS (2014), Dubai CS (2017)	NCS (2013)	NCS (2014)	e.Oman (2003), revised 2010	NCS (2017)	NCS (2017)

Abbreviations:
MCIT: Ministry of Communications and Information Technology
NTRA: National Telecommunications Regulatory Authority
MTC: Ministry of Transport and Communications
CAIT: Central Agency for Information Technology
CIO: Central Informatics Organisation

CITC: Communications and Information Technology Commission
TRA: Telecommunications Regulatory Authority
ITA: Information Technology Authority
CITRA: Communication and Information Technology Regulatory Authority
HCCS: High Council for Cyber Security
NESC: National Electronic Security Council
NESA: National Electronic Security Agency
CSC: Cyber Security Centre
NSC: National Cybersecurity Strategy

I now detail the appropriation of cybersecurity between these organisations in each state in turn.[502]

First, as the table above indicates, Oman created cybersecurity organisations within IT and telecoms departments in 2010. The Omani organisation was branded internally as 'the national centre for cyberpeace' (*al-markaz al-watani lil-salam al-sibrani*), and outwardly as a CERT (Oman CERT or OCERT), while one interviewee called it the 'National Cyber Security Centre' (NCSC). They explained its function as follows:

> We work closely with the Cabinet and the National Security Agency, promoting cybersecurity. The same minister is chairman of both ITA and TRA, and we have representatives of security and intelligence agencies on our board, we are also engaging local law enforcement. There is a government committee, and we have been given the authority to do cybersecurity. We have direct contact with national security agencies, and we present to them from time to time when requested. The NCSC is seen as a neutral organisation, unlike police or law enforcement (I-1).

Other interviewees disagreed with this portrayal somewhat dismissively, with one saying that "OCERT is just an awareness and PR role" (I-34). Others highlighted the role of the security agencies, with one interviewee noting that in cybersecurity "there are the Royal Office, and then the ISS [Internal Security Service]" (I-27) and another summarising the Omani cybersecurity landscape as "the Royal Office, protecting government departments, the ISS with a wider remit including CNI, while ITA do education" (I-42). Finally, a UK national claimed that "ISS will be the national cyber lead, charged with delivering national security in cyber… there is friction caused by different agencies in the same space" (I-46). These interviews suggest that cybersecurity responsibility was appropriated by the Omani security agencies from the NCSC, despite the 'friction' this caused.

[502] Other than Kuwait, due to the research constraints in Chapter 4.

In Qatar, the key role of intelligence agencies and interior ministries was stressed by a Qatari national with extensive experience in the Qatari government:

> The role of the MOI [Ministry of Interior] is to combat cybercrime. Defence against aggression, and so cyber aggression – it's simple, you add cyber. They also retaliate. Intelligence agencies do lots of counter intelligence, so add cyber and they do cyber counter intelligence (I-4).

This 'division of labour' view of cybersecurity leaves no room for the Qatar CERT (QCERT), based in the IT ministry. The other interesting part of the quotation above is the off-hand comment about MOIs that "they also retaliate", meaning that they conduct cyberattacks and surveillance operations. Another interviewee also addressed the matter of offensive capability, stating that:

> I can't word it in a politically correct way, everyone wants to avoid and protect against attacks, but they are also considering offensive capabilities. You can't have it both ways… In QCERT we have capabilities for reverse engineering and malware analysis, which puts us in a unique position. Maybe there are other agencies in Qatar that can do this, but we are the oldest and have never been approached (I-53).

In this quotation the interviewee puts forward a justification for the inclusion of QCERT in the development of 'offensive capabilities'. However, as they recognised, the Qatari Ministry of Interior did not involve QCERT in its search for ways to 'retaliate'. Instead, it purchased surveillance technology from private companies including Finfisher and ETI, and probably also contracted out targeted surveillance to monitor labour and immigration activists. The institutional appropriation of cybersecurity by MOIs and security agencies thus includes not only the passive protection of networks, but also the use of 'offensive' capabilities.

The cybersecurity organisations in the UAE illustrate similar patterns of appropriation. The creation of the UAE National Electronic Security Agency (NESA) was first announced in 2012.[503] However, this supposedly nationwide organisation was not operational for another two years,[504] and its authority was immediately challenged by the creation of a separate Electronic Security Centre in

[503] Awad Mustafa, 'UAE Leads the Way in Cyber Security', The National, 25 February 2014, https://perma.cc/8GYK-2FTL.
[504] Stephen McBride, 'UAE Cyber-Security Authority Unveils Policies, Standards', ITP.net, 25 June 2014, https://perma.cc/HF7X-VFH5.

Dubai in 2014 (including entirely separate cybersecurity standards).[505] The UAE then announced its intention to create a military cyber command in September 2014, bringing another powerful player into the cybersecurity arena. According to media reports, when operational it will run 'in parallel' with NESA.[506] These overlapping authorities effectively sideline the Telecommunications Regulatory Agency (TRA), even though the TRA is the base for the national CERT (aeCERT).

These movements also reflect the federal structure of the UAE and competition between the two ruling families of the wealthiest emirates, Dubai and Abu Dhabi. The UAE political system necessitates close connections to members of the ruling families, which one interviewee claimed were possessed by NESA: "For NESA, the CEO is very close to the crown prince, and so they have authority from the top. For example, a ministry wouldn't implement it [the UAE cybersecurity regulation] so he got a call [from the crown prince]." (I-2). For context, the Director General (described by the interviewee as the CEO) of NESA was Jassem Bu Ataba Al-Zaabi, from a family with connections to the ruling family of Abu Dhabi, while the Crown Prince of the UAE, a position held by the Abu Dhabi ruling family themselves, was Sheikh Muhammad bin Zayed Al-Nahyan. Their close relationship was mentioned as shaping cybersecurity governance in the UAE.

As with Qatar, protective capabilities overlap significantly with intelligence gathering. Another interviewee suggested that the creation of NESA was as much about intelligence ownership as cybersecurity control. In their words:

> The UAE decided to set up… NESA… they had some key people in government and industry for this, the government people came from the MOI and the MSS [Ministry of State Security]… SIGINT came together in NESA. SIGINT was already in MOI, so NESA said yes keep it, but as a service. We will provide that service to you and others e.g. MFA [Ministry of Foreign Affairs]. (I-49).

This centralisation of SIGINT shows how the movement of individuals is crucial for appropriation, as people were recruited from the MOI and MSS for the creation of NESA. This SIGINT role of NESA is not mentioned in any official sources; nonetheless, if the interviewee is correct, then NESA

[505] Andy Sambridge, 'Dubai Sets up E-Security Centre to Fight Cyber Criminals', ITP.net, 13 June 2014, https://perma.cc/F7LX-R2VZ.
[506] Thomas Bindiya, 'UAE Military To Set Up Cyber Command', Defense World, 30 September 2014, https://perma.cc/VP7F-EEXF.

has used the political capital of cybersecurity to acquire intelligence capabilities. As seen in the previous chapter, these capabilities are used by actors probably working in or for the UAE government to track dissidents and human rights activists. Overall, the creation of NESA indicates an institutional appropriation of cybersecurity, privileging intelligence and national security operations over telecoms agencies.

In Saudi Arabia, cybersecurity developed in the shadow of the royal succession, as King ʿAbdullah died in 2015, succeeded by his brother Salman and King Salman's son Muhammad bin Salman. The rise of Muhammad bin Salman pushed other branches of the Saudi royal family away from key positions, including Muhammad bin Nayef, who had been first Assistant Minister and then Minister of the MOI and a longstanding partner for Western intelligence agencies. Until his removal from power in 2017, bin Nayef and the MOI were key actors in cybersecurity governance in Saudi Arabia. Under Nayef, the Ministry of Interior showed an early interest in cybersecurity. According to a leaked US cable, in 2009, the MoI invited a US expert to brief the specialist MOI university (the Nayef Arab University for Security Sciences) on cybersecurity. The cable stated that:

> NAUSS' interest in cyber security assistance reflects the high priority the Saudi Ministry of the Interior (MOI) places on this subject. The MOI separately requested US assistance with a new cyber security program in May of this year.[507]

This early focus on cybersecurity in the MOI continued after the Arab Spring and the Shamoon incident. At the first national cybersecurity forum in 2013, the director of the national cybersecurity programme at the MOI, ʾAbd Al-Rahman Al-Muʿaiqil, announced the creation of a national cybersecurity centre.[508] In a statement at this forum, the newly appointed director of the centre itself, Dr Salih Al-Mutairi, mentioned that they would aim to share information with sectors including telecoms.[509] Thus at the start of government movements towards cybersecurity in Saudi Arabia, the

[507] Wikileaks, 'US Embassy Riyadh - Saudi Arabia: New Opportunities for Assistance with Naif Arab University' (Wikileaks Public Library of US Diplomacy, 31 August 2009), Public Library of US Diplomacy, https://perma.cc/FCF6-KT4Z.

[508] ʿAbdallah Al-Khalifi, 'Al-Saʿudiyya Tadrusu ʾinshaʾ Hayaʾat Wataniyya Liʾamn Al-Muʿalumat [Saudi Arabia Studies the Formation of a National Centre for Information Security]', Al-ʿArabiyya, 18 June 2013, https://perma.cc/9CEG-XHP9.

[509] Nasir Al-ʿAli, 'Markaz Watani Lil-ʾamn Al-ʾiliktruni Limuwajihat Al-Ikhtiraqat Wa Al-Hujumat Al-ʿaliyya Al-Taʿqid Lilbana Al-Tahtiyya Al-Istratajiyya [National Centre for Electronic Security to Confront Hacks and Attacks of Increased Complexity against Critical Infrastructure]', Al-Iqtisadiyya, 27 June 2013, https://perma.cc/JMH9-R9VB.

MOI was clearly the catalyst more than telecoms regulators or IT agencies, despite an image of seamless national government collaboration.[510]

The central role of the MOI in creating cybersecurity institutions in Saudi Arabia was explained by one interviewee as follows:

> After Aramco, there was a Royal Decree that major ministries had to have an infosec [information security] department. But there was no cybersecurity strategy, just an instruction. If you were in Education, you'd implement differently to MOI or MOD. The Air Force, the Navy, both wanted a SOC [a Security Operations Centre], then MOD wanted a SOC above them, then MOI wanted a SOC that protected the nation as a whole – it monitored the internal gateway… Then the concept of converging SIGINT and cyber missions emerged. If you already have the capability (DPI, monitoring, etc) then why spend millions on new ones? (I-49)

This quotation indicates that, in Saudi Arabia as in the UAE, intelligence and cybersecurity overlapped significantly due to overlapping technological capability. However, the interviewee also revealed how the concept of cybersecurity became synonymous with a broad definition of national security, as the SOC "protects the nation as a whole". Even the term SOC here is expanded beyond its original meaning as the cybersecurity centre for an organisation, to signify cybersecurity responsibility for the state as a whole. This quotation suggests that institutional, technological, and conceptual appropriation all reinforced the MOI's appropriation of cybersecurity in Saudi Arabia.

However, this ownership has limits. Both the Ministry of Defence and the National Guard - separate organisations run by separate branches of the royal family until the consolidation of power in 2017 - have procured sophisticated military technologies for electronic warfare.[511] A UK national and former contractor to these organisations described their focus as follows: "Saudi Arabia are now doing ops in Yemen, and they want to use cyber to derisk those military operations, with GCHQ like capabilities. They are doing social media monitoring, and covert ops like JTRIG [the GCHQ 'cyber operations' department]" (I-47). The social media monitoring capabilities mentioned here are very

[510] MCIT (Saudi Arabia), '20 Government Agencies to Participate in National Information Security Program (Amen)', Ministry of Communications and Information Technology, 17 January 2016, https://perma.cc/YE3G-MKWY.

[511] Al-Defaiya, 'Saudi Arabia to Host Electronic Warfare Symposium', 18 October 2013, https://perma.cc/5E6S-4HEZ; Oxford Business Group, 'Enhancing Saudi Arabia's Cybersecurity Readiness', Oxford Business Group, 29 September 2015, https://perma.cc/AAU2-RGMN.

similar if not identical to those acquired by the MOI in the earlier quotation, suggesting that such 'cybersecurity' technologies are duplicated across the Saudi government.

The central role of the MOI has also been affected by political shifts in Saudi Arabia. A new national cybersecurity centre was created in November 2017 under a member of the Ministers' Council, Dr Musaʿid Al-ʿAiban. This centre had a wider executive council, including the heads of General Intelligence and State Security and only the deputy and assistant ministers for Interior and Defence respectively. This shift towards the intelligence agencies followed Muhammad bin Salman's removal of Muhammad bin Nayef earlier in the year, and Al-ʿAiban specifically thanked Muhammad bin Salman for his appointment.[512] The appropriation of cybersecurity by the MOI was thus also curtailed by sudden shifts in the domestic political landscape.

In Bahrain, interviewees noted the influence of international partners, including the UK, in the institutional competition between telecoms, security agencies and the MOI. As one interviewee stated, "the UK government has been trying hard to help them have the capability to track networks, this capability has been given to the NSA [the Bahrain National Security Agency], not the MOI. This is part of the reason for arrest and detention going back to the NSA." (I-33).

The decision here by the UK to provide SIGINT or 'cybersecurity' capability to the NSA rather than the MOI was attributed by this interviewee to the human rights violations committed by the MOI in its suppression of protests after the Arab Spring. This interviewee thus portrayed the UK as balancing its intelligence partnership with Bahrain on one hand with human rights concerns around that partnership on the other. This calculation by exporting states and companies such as the UK will be examined further in the next chapter. Here, I note only that telecommunications ministries were not a significant presence, suggesting a similar pattern of appropriation. As an interviewee in the Bahraini telecoms regulator said: "they take care of things themselves. What happens in national security we are oblivious to it, we don't know what functionality they have" (I-55).

Finally, I turn to Egypt. Although the Egyptian CERT and the Ministry of Communications and Information Technology within which it was located had played a key role in cybersecurity

[512] Staff Report, 'ʾamr malaki biʾinshaʾ "al-hayaʾat al-wataniyya lil-ʾamn al-sibrani" [Royal order to create the "National Centre for Cybersecurity"]', Al-ʿArabiyya, 1 November 2017, https://perma.cc/KFB3-9JLP.

governance since at least 2009, as detailed in Chapter 3, cybersecurity was lost in the turmoil engulfing Egypt after the January 2011 revolution. After President Al-Sisi won highly manipulated elections in May 2014, he created a High Council for Cyber Security including defence and foreign ministries, intelligence agencies, and the MOI as well as the MCIT. Activists highlighted the involvement of intelligence agencies and MOI as indicative of Al-Sisi's increasing repression.[513] Specific arguments included the vagueness of the Council's purpose and the necessity for the participation of intelligence agencies if surveillance was not part of its remit. [514] As the above exploration of the GCC states - who provided significant financial and political support to Al-Sisi's government – has shown, the two cannot be clearly distinguished: SIGINT, national surveillance and offensive capabilities all became part of cybersecurity as the institutional interests behind cybersecurity structures gravitated towards domestic security concerns.

This appropriation of cybersecurity in Egypt can be seen clearly by comparing the activity of the High Council to that of the MOI, which was ostensibly part of this wider cybersecurity framework. The High Council was barely active for three years after its creation in December 2014. A year after its creation, an influential Egyptian cybersecurity expert, ʿAdel ʿAbdel Moneim, suggested publicly that the council was frozen and needed to act quickly.[515] The High Council did eventually meet after the global outbreak of the Wannacry ransomware virus in February 2017.[516] However, despite the High Council's paralysis, the MOI was extremely active in 'cybersecurity' during this time. I noted in the previous chapter that the surveillance and traffic monitoring companies Blue Coat, Narus, and Gamma International all reportedly competed for a government social media monitoring contract tendered in Egypt in 2014. Discussions of this tender in the

[513] Zeinab El-Gundy, 'Founding of State Cyber-Security Body Worries Digital Rights Activists', Ahram Online, 19 December 2014, https://perma.cc/HTB3-P897.
[514] Amr Abdelatty, 'Egypt's Cybersecurity Council Prompts Privacy Concerns', Al Monitor, 15 January 2015, https://perma.cc/D4Z7-NC9M. Staff Report, '"Al-Majlis Al-ʿali Lil-ʾamn Al-Sibrani" ʾam Al-Majlis Al-ʿali Lil-Raqaba? [The "High Council for Cybersecurity" or the High Council for Surveillance?]', Al-ʿArabi Al-Jadid, 18 December 2014, https://perma.cc/M3TG-4BYC.
[515] Ahmad Majdi, 'Khabir ʾamn Al-Muʿalumat Yutalibu Bitafʿil Al-Majlis Al-ʿali Lil-ʾamn Al-Sibrani [Cybersecurity Expert Suggests Activating the High Council for Cybersecurity]', Mubtada, 8 August 2016, https://perma.cc/DS52-T446.
[516] Sanaʾ ʿAbd Al-Wahhab, 'Al-Majlis Al-ʿali Lilʾamn Al-Sibrani Yajtamiʿu Limutabiʿat ʾakhar Tatawarat "Firus Al-Fidiyya" [The High Council for Cybersecurity Meets to Follow the Latest "Ransomware" Developments]', Al-Masry Al-Youm, 15 May 2017, https://perma.cc/4N22-65UR.

Egyptian press point to a leaked call for a surveillance system for social media in June 2014 issued by the MOI.[517] Amnesty International claimed that this system would be used for human rights violations; this is likely given the wider practices of the Egyptian security apparatus.[518]

Claims of mass surveillance were denied by those responsible for the tender, as an MOI official claimed it was for "electronic crimes" (*al-jaraʾim al-ʾiliktruniyya*) and would only be used to monitor terrorists.[519] This was, typically, met with social media satire on Twitter, using hashtags including 'we are censored/surveilled' (*ihna mutaraqabin*) and "direct message to your private agent" (*wajjaha risala lil-mukhbirak al-khas*).[520] Furthermore, this surveillance system was probably a necessary technological precondition for the activities of a committee formed in February 2015 to recommend how to remove any content linked to terrorism from Egyptian websites.[521] Following its formation, online censorship and website blocking – of all kinds, including liberal websites not affiliated with the Brotherhood or any Islamist group - increased significantly.

A media interview with Sabri Saʿad, Head of the General Directorate for Information and Documentation at the MOI at the time of the formation of the Council, underlines the broad definition of national security underpinning the MOI's view of cybersecurity. In this interview, Saʿad used the concepts of cybercrime and terrorism interchangeably: in one passage, he stated that "the struggle against electronic criminals is like a game of chess" (*mukafahat al-jaraʾim alʾiliktruniyya ʾashbaha bi laʿabat shatranj*) whereas elsewhere he used the chess game simile in "waging war on [Muslim] Brotherhood militias" (*nuharibu milishiyyat alʾikhwan wa kaʾanana nalʿabu shatranj*).[522] Saʿad's

[517] Majdi Al-Jalad, 'Infirad: Al-Dakhiliyya Tafridu "Qabda ʾiliktruniyya" ʿala Jaraʾim Shabakat Al-Tawassul Al-Ijtimaʿi [Exclusive: The Ministry of the Interior Imposes "Electronic Grip" on Social Media Crimes]', Al-Watan, 1 June 2014, https://perma.cc/TCE3-N26A.
[518] Amnesty International, 'Egypt's Plan for Mass Surveillance of Social Media an Attack on Internet Privacy and Freedom of Expression', Amnesty International, 4 June 2014, https://perma.cc/YFY3-KTQ2.
[519] Muhammad Shuman and ʾIshraf Hazaʿ, 'Mudir Mubahith Al-ʾintarnit: Narsudu Al-ʾirhabiyyin Wa La Natajassasu ʿala Al-Muwatinin [Director of Internet Research: We Observe Terrorists and Do Not Spy on the People]', Al-Ahram, 5 June 2014, https://perma.cc/P3UP-CXHE.
[520] Muhammad Kasab, 'Sukhria Min Raqaba Al-Dakhiliyya Limauqiʿat Al-Tawassul [Sarcasm over Government Surveillance of Social Media Sites]', Al-Masry Al-Youm, 3 June 2014, https://perma.cc/S8AP-KGAZ.
[521] Ahram Online, 'Egypt to Block Websites Linked to "Terrorism"', Ahram Online, 17 February 2015, https://perma.cc/RLJ3-LMCR.
[522] Muhammad Barakat, 'Musaʿid Wazir Al-Dakhiliyya Li "Muʿalumat Wa Al-Tawthiq": Nuharibu Milishiyyat Alʾikhwan Wa Kaʾanana Nalʿabu Shatranj [Assistant Minister of Interior for "Information and Authentication": We Fight Brotherhood Militias as If We Are Playing Chess]', Al-Watan, 28 February 2014, https://perma.cc/7W5X-TR9A.

robust defence of social media surveillance, combining the vocabulary of cybercrime and terrorism, is a clear appropriation of cybersecurity.

In sum, in this section I have argued that throughout Egypt and the Gulf states cybersecurity was appropriated by MOIs and state security agencies, especially after the Arab Spring. This was based on the dual-use possibilities of some technologies for both countering cybersecurity threats and large-scale surveillance of national internet traffic and social media. This overlap meant that MOIs and security agencies used cybersecurity as a justification for obtaining and retaining sophisticated surveillance capabilities, while also moving the domain of cybersecurity itself towards their own invested aim of suppressing political opposition.

***

This chapter has traced the moral manoeuvre of appropriation by actors invested in an expansive definition of national security, and has demonstrated how this moral manoeuvre differs from accounts of norm resistance and localisation. Although norm-based explanations gesture towards the complex environment of differing goals and shifting meanings detailed in this chapter, they focus on particular agreements (e.g. the Budapest Convention), rather than prioritising the invested motivation of specific actors *within* state structures, who see international agreements as just one element in their efforts to enforce an expansive definition of national security. This chapter has also put appropriation in the context of the rights-based view of cybersecurity in the previous chapter. Specifically, the appropriation of cybersecurity by governments in Egypt and the Gulf states inverted rights-based views of cybersecurity, with the exact individuals who defended human rights against the threat of government surveillance in the latter instead occupying the position of threat to the state in the appropriated version. In the next chapter, I examine how surveillance suppliers perform a third moral manoeuvre between these conceptions of cybersecurity: manipulation.

Chapter 8. Manipulation

> To whom may still believe that values and ethics do apply at that level... National security and fighting terrorism is done by being utterly realistic. Being utterly realistic – that's life, that's realpolitik.[523]
>
> (Internal email forwarded with approval by the CEO of Hacking Team.)

After Citizen Lab reported the association of human rights violations with surveillance technologies sold by the Italian company Hacking Team, Hacking Team drafted a response to an enquiry from the Washington Post with the following message: "We share with Citizen Lab a concern for human rights throughout the world, but we share with law enforcement authorities around the world a concern that the Internet and mobile technologies can be used for criminal activities as well as for good".[524] This was clearly a publicity line, written as part of a defensive response to media questions. However, its profession of concern for both human rights and national security concerns is interesting, given that the moral manoeuvre detailed in the previous chapter showed how these two conceptions of cybersecurity are inverted in Egypt and the Gulf states. How do companies that manufacture and sell surveillance technologies reconcile the two clusters of values referenced by Hacking Team?

This chapter examines a third set of actors in cybersecurity in Egypt and the Gulf states: the suppliers of surveillance technologies to governments. These suppliers include both the private companies making such technologies and the states that export them. Exporting states support and licence individual companies and contracts, with cybersecurity and surveillance exports fitting within wider diplomatic and economic relationships. Both public and private sectors overlap significantly in technologically advanced surveillance industries that require high levels of skill and a significant defence industrial base; hence the description of a 'cyber-industrial complex'.[525]

---

[523] Wikileaks, 'Hacking Team Email-ID 11899', 29 May 2015, https://perma.cc/NRA9-8JPA.
[524] Wikileaks, 'Hacking Team Email-ID 149888', 12 August 2014, https://perma.cc/QS2F-53KW.
[525] Martin Stabe, Steve Bernard, and Marissa Oberlander, 'The New Cyber-Industrial Complex', *Financial Times*, 10 October 2011; Staff Report, 'Meet The Cyber-Industrial Complex: Private Contractors May Get $7B Windfall From Pentagon's Cyberwar On ISIS', International Business Times, 7 March 2016, https://perma.cc/SQ4S-8MEM; Ronald J. Deibert and Rafal Rohozinski, 'The New Cyber Military-Industrial Complex', The Globe and Mail, 28 March 2011, https://perma.cc/PJL9-AKGU.

This chapter argues that these companies perform the moral manoeuvre of *manipulation:* the renegotiation of value and technical concepts to assimilate separate value clusters without a specific normative commitment. This agnostic motivation distinguishes surveillance suppliers, who see themselves as primarily motivated by profit, from both the NGOs considered in Chapter 6 and the states considered in Chapter 7. Both NGOs and states were invested in specific values or clusters of values: for NGOs, the promotion of human rights, and for government organisations, an expansive definition of national security. In contrast, surveillance suppliers manipulate both national security and human rights values to increase sales, rather than striving to promote these values themselves. The key element of this moral manoeuvre is flexibility, ensuring that values are amendable through structures of abuse and misuse and wider risk calculations.

The alternative norm-based explanation of this phenomenon – as companies' reaction to an emerging norm of the amended Wassenaar Arrangement on Dual Use Technologies – does not explain how both exporting states and companies are able to comply with the Wassenaar Arrangement and yet maintain their prior sales practices. This is especially true for those states who proposed the amendment, such as the UK, undermining a simple view of this action as norm entrepreneurship. The 'continuum of norm acceptance' considered in Chapter 2 is replaced here by a flexible manipulation of values, where companies and states move easily between acceptance and resistance, favouring the restriction of surveillance technologies or their proliferation at different times and for different clients. The point is not that socialising target actors to 'internalise' a norm can only go so far, but that the process of socialisation *itself* can be manipulated by these actors.

This chapter has three sections. The first section explores the movement of multinational defence companies - with a large presence in Egypt and the Gulf states - into cybersecurity. The second section examines how surveillance suppliers such as Hacking Team incorporated human rights values into their sales structures. The third section focuses on exporting states, using the example of the UK, investigating the way export control mechanisms facilitate as well as restrict surveillance sales.

8.1 Defence companies in cybersecurity

This section argues that surveillance suppliers to Egypt and the Gulf states are heavily entangled in the wider defence sector and retain these links due to difficulties in transplanting their expertise and technologies into commercial environments. This is the basis for the moral manoeuvre of manipulation, as these companies draw on their wider understanding of the purpose and values of defence industries to justify sales of surveillance equipment.

Many defence companies have established a longstanding and lucrative presence in Egypt and the Gulf due to the strategic significance of these states and their proximity to severe conflict. This presence is a key advantage in cybersecurity and surveillance markets. This is partly due to the simple fact that defence companies have a privileged position in crucial national security circles and extensive connections in militaries and security agencies.[526] However, it is also due to their involvement in the industrial sectors of these states through what are known as 'offset' agreements. Offsets are arrangements, often negotiated at a state level, in which the price of arms is 'offset' by investment in local industry. Offsets distort 'natural' markets both in the arms sector and in the sectors in which offset investment is made.[527] This practice is widespread across Egypt and the Gulf states, sometimes including digital start-ups.[528] Together, elite connections and their offset-enabled economic weight mean that multinational defence companies are a central element of state security architectures.

The biggest defence companies have diversified into cybersecurity over the last decade.[529] They justified this move because "the boundary between the defence world and the non-defence world in cyberspace blurs", according to French company Thales.[530] US company Lockheed Martin

[526] Bilal Y. Saab, 'The Gulf Rising: Defense Industrialization in Saudi Arabia and the UAE' (Brent Scowcroft Center on International Security at the Atlantic Council, May 2014).
[527] Ron Matthews, 'The UK Offset Model: From Participation to Engagement', *RUSI Whitehall Report*, 29 July 2014.
[528] Gulf Industry, 'Interactive Saudi Arabia Opens Offices', *Gulf Industry* 13, no. 2 (March 2004), https://perma.cc/HT9S-FGVP.
[529] Vincent Boulanin, 'Cybersecurity and the Arms Industry', in *SIPRI Arms Yearbook 2013* (Oxford: Oxford University Press, 2013), 218–26.
[530] Zachary Fryer-Biggs, 'Defence Companies Try to Tackle Commercial Cyber Market', *Jane's Defence Industry* 32, no. 5 (1 May 2015).

described their cybersecurity ventures as an attempt to provide commercial 'door-opener' in a time of decreasing arms sales worldwide in the late 2000s.[531] Their director commented further on the benefit of having a cybersecurity business, saying that "we move people back and forth, we share intelligence".[532] This suggests that cybersecurity is not merely an external addition for these companies, but a source of data improving their core business.

However, defence companies' movement into cybersecurity has not always been smooth. The defence publication Jane's suggested that many cybersecurity acquisitions failed due to "the complications of running a commercial business based upon company investment within defence organisations accustomed to single customer government needs".[533] Similarly, an analysis in the Financial Times claimed that "defence companies struggle when they go head to head with some of the software specialists. They don't seem to be good at . . . making it repeatable — out of the box and easy to use."[534] These reports indicate that, despite the advantages possessed by defence companies, the high level of competition and requirement for immediate results – both characteristics that cybersecurity shares with digital technology sectors, rather than traditional security sectors – mean that cybersecurity is not merely an extension of older intelligence and surveillance contracts.

These difficulties were noticed by some interviewees in Egypt and the Gulf states. For example, one interviewee described the role of defence companies as follows:

> Defence companies waded into cybersecurity, buying businesses they didn't really understand… The problem was that you need a client-side relationship. But the culture changed once [the defence company] took over, and you started to lose clients because this fell away. People were incentivised to sell units. You needed to be an intermediary rather than a salesman. (I-42)

For this interviewee, the differences between the business culture of defence companies and cybersecurity companies were stark. It was these social differences, rather than the technical details of cybersecurity, that meant cybersecurity companies functioned in a way defence companies "didn't

[531] Andrea Shalal-Esa, 'Lockheed Aims to Conquer Markets Outside U.S.', *Reuters*, 21 June 2013, https://perma.cc/Z22S-AB8G.
[532] Fryer-Biggs, 'Defence Companies Try to Tackle Commercial Cyber Market'.
[533] Fryer-Biggs.
[534] Peggy Hollinger, 'Defence Groups Take Aim at Cyber Security', Financial Times, 28 March 2016, https://perma.cc/AQY8-DTGQ.

really understand". However, this interviewee also noted that defence companies adopted a range of strategies, sometimes successfully connecting traditional defence sales and cybersecurity:

> But BAE and Raytheon gave themselves depth. For example, when they sell the Typhoon, what will they do with the data from sensors? It opens opportunities for cyber capability without trying to ram it down people's throats. (I-42).

Here, the interviewee highlights how some defence companies managed to integrate 'cyber capabilities' into their existing arms sales. As this interviewee recognises, both UK-based BAE Systems and US-based Raytheon have long relationships with Egypt and the Gulf states and are key parts of the cybersecurity and surveillance industries in this region. It is therefore worth examining their trajectories in cybersecurity more closely.

Raytheon acquired many companies to move into the cybersecurity market. Between 2007 and 2012, it bought eleven cybersecurity companies.[535] This new cybersecurity market included the Gulf, where a spokesman said that "we have moved aggressively into what we call adjacencies such as homeland security and cyber security". An early example of its involvement in cybersecurity in the region was the sale of cybersecurity solutions for UAE critical infrastructure in 2010.[536] Raytheon continued to make cybersecurity acquisitions after 2012, including its biggest purchase, Websense, in 2015 for just under $2 billion.[537] Websense had its own history in the region, having bidded for the rights to provide filtering software in Saudi Arabia in 2001 as noted in Chapter 3. Raytheon then integrated Websense into 'Forcepoint', a separate cybersecurity branch.

Jane's noted how this series of acquisitions distinguished Raytheon from its competitors, stating that: "Raytheon has been by far the most aggressive US defence company in its efforts to take its cyber security presence and expand into the commercial market, although a number of other companies have tried."[538] Unsurprisingly, the Raytheon CEO claimed that their long history in the region was the main factor that enabled them to move into cybersecurity:

---

[535] Charles Forrester, 'Raytheon Expands Cybersecurity Stable', *Jane's Defence Industry* 29, no. 11 (1 November 2012).
[536] UAE Government News, 'Raytheon in Talks With UAE to Make Security Deal' (Contify, 21 July 2010).
[537] Charles Forrester, 'Raytheon Announces Billion-Dollar Cyber Acquisition', *Jane's Defence Industry* 32, no. 5 (1 May 2015).
[538] Zachary Fryer-Biggs, 'Raytheon to Buy Stonesoft', *Jane's Defence Industry* 32, no. 12 (1 December 2015).

> In Saudi Arabia at that time – we had been there 47 or 48 years – we leveraged our partnerships in country, and the work we'd done, to grow beyond those customers we already had. If you've been in a country for many years, there's a lot you learn – culture, how they do business, how they do acquisitions."[539]

The best example of Raytheon 'leveraging its partnerships' to include national surveillance is in the UAE. According to an Intelligence Online report, Raytheon's 'Intelligence and Information Systems Division' has played the role of 'integrator' for the UAE National Electronic Security Agency (NESA) since its founding in 2012.[540] As demonstrated in the previous chapter, NESA occupies a dual role between cybersecurity and national surveillance, both setting cybersecurity standards and providing monitoring capabilities to other government agencies. Although Raytheon was the main contractor for the UAE government, this report suggests that Raytheon subcontracted much of the work to US technology company Cisco and US defence company Booz Allen Hamilton (BAH), and that US company Verint later took over the contract. Raytheon has thus diversified into cybersecurity in both commercial settings and as an extension to existing national security contracts, including surveillance.

As well as providing cybersecurity services under Raytheon's overall management, BAH has also been involved in negotiations to sell 'offensive' cyber capabilities in the region. In 2012, the Washington Post reported that the Qatari government contracted Booz Allen Hamilton to provide a cyber operations centre to conduct hacking operations against its regional adversaries. According to the Post's unnamed national security sources, this request was not fulfilled because the US military were reluctant to allow US personnel to staff the centre due to the potential negative repercussions from their involvement.[541] If correct, this report illustrates both the close engagement of the US government in these transactions, and the extensive overlap between suppliers of defensive and offensive cyber capabilities.

---

[539] Jill Aitoro, 'Q&A: Raytheon CEO on Calls for Sovereignty, Moving Past Wars of Insurgency', Defense News, 11 July 2016, https://perma.cc/RQP7-L5P7.
[540] Intelligence Online, 'Verint Poised to Land Major Emirates Interceptions Contract', 18 October 2017, https://perma.cc/W6Q9-M6G5; Intelligence Online, 'Abu Dhabi's NSA and Its Helping Hands', 5 April 2017, https://perma.cc/PTH3-AYXU.
[541] Ellen Nakashima, 'As Cyberwarfare Heats up, Allies Turn to U.S. Companies for Expertise', Washington Post, 22 November 2012, https://perma.cc/WNP6-UUS3.

The other company with extensive cybersecurity operations across the Middle East is BAE Systems. BAE has an especially long history in the Gulf states, including a deep understanding of what the Raytheon CEO termed 'how they do business' in arms sales. In particular, BAE's 'Al-Yamamah' sales of fighter jets to Saudi Arabia in the 1980s and 1990s were followed by extensive reports of corruption.[542] These reports culminated in the opening of a Serious Fraud Office investigation in 2003, although it was cancelled in 2006 by Prime Minister Tony Blair due to national security concerns.[543] This history reinforces the unique set of economic and political relationships in which BAE continues to operate. Its regional director emphasised these local ties in 2012, saying that "BAE is a Saudi company, and is becoming more so".[544]

BAE has conducted many cybersecurity acquisitions, including its main cybersecurity subsidiary, Detica, in 2008 for just under $1 billion. In 2014 it rebranded Detica as 'Applied Intelligence'.[545] In 2015 BAE completed the purchase of cybersecurity company Silversky, integrating Silversky under Detica in the wider 'cyber and intelligence' group within BAE.[546] BAE's move to commercial cybersecurity mainly focused on its analysis product, NetReveal.[547] Originally designed for intelligence analysis, this software was then marketed to both governments and commercial clients. As an interviewee explained, "Their data analysis product was Netreveal... then they made CyberReveal, and bespoke products. But you need a commercial product for international governments and companies. CyberReveal did cyber monitoring, large scale data" (I-25). Consequently, BAE focused its attention in the region on financial cybersecurity threats.[548] This

[542] David Leigh and Rob Evans, 'BAE and the Saudis: How Secret Cash Payments Oiled £43bn Arms Deal', *The Guardian*, 5 February 2010, https://perma.cc/2QP7-NLH2.
[543] Michael Peel, 'How the Inquiry into BAE's Saudi Deals Was Brought to Earth', *Financial Times*, 25 February 2007.
[544] Walaa Hawari, '"60 Percent of Work Force in BAE Systems Are Saudis"', Arab News, 15 January 2012, https://perma.cc/M85V-6NET.
[545] Guy Anderson, 'Detica to Rebrand as BAE Systems Applied Intelligence', *Jane's Defence Industry* 31, no. 2 (1 February 2014).
[546] Guy Anderson, 'BAE Systems Announces Eclipse Electronic Systems Acquisition and Closure of SilverSky Deal', *Jane's Defence Industry* 32, no. 1 (1 January 2015).
[547] ENP Newswire, 'Bank of Sharjah Implements BAE Systems NetReveal' (Electronic News Publishing, 29 December 2015).
[548] Banker Middle East, 'Business Defence Forum: The Compliance Front Line' (SyndiGate Media Inc., 21 November 2016).

caused new problems, as one interviewee explained with regards to the 2013 Bank Muscat fraud mentioned in Chapter 5:

> At the time of the hack BAE had two products on the table of the CIO [Chief Information Officer] and the head of risk management respectively. One was a cybersecurity product aiming to detect insider threat through vetting… The other product was Netreveal – an anomaly detection product for fraud. After the Bank Muscat hack BAE thought 'clearly they are going to buy these now'. But Bank Muscat said it was within tolerance. The publicity was a problem, but the amount was not significant enough for them to change their priorities. Bank Muscat tended to invest in solutions that maintained compliance, but they had a different risk appetite (I-42).

This interviewee suggests that, just like other defence companies, BAE encountered significant problems moving into commercial cybersecurity. Although it acquired a company with a product that straddled both intelligence analysis for governments and commercial cybersecurity requirements, the different risk calculations in these environments meant that BAE was unable to move easily between them. Consequently, BAE's sales of national-level surveillance equipment, such as those by its subsidiary ETI to Oman, Qatar, Saudi Arabia and the UAE noted in Chapter 6, remained a strategically important part of its overall sales, even if total returns were dwarfed by more traditional arms.

As well as defence companies such as BAE and Raytheon, smaller surveillance suppliers examined in Chapter 6 like Hacking Team, Finfisher, and NSO Group also have links to traditional defence industries. NSO Group are one of many cybersecurity and surveillance companies to emerge from the Israeli military, especially their signals intelligence department Unit 8200. Finfisher's original parent company, Gamma International, was owned by an individual named Louthean Nelson, an arms dealer based in Beirut with connections to many defence companies.[549] Around the time of the Wassenaar amendment, and after complaints submitted by Privacy International to the OECD and various UK government bodies, Gamma International separated from FinFisher, which is at the time of writing a separate company based in Germany. Hacking Team also operate in a

[549] Buro Jansen & Jansen, 'Gamma Group/Louthean Nelson; Arms Dealers Pur Sang', 19 January 2017, https://perma.cc/V6RN-7XMX.

complex supply chain, with local resellers on one side and defence companies providing complementary capabilities on the other.[550]

In sum, cybersecurity is heavily entangled with surveillance and analysis technologies in the broader defence sector. Although this is partly due to the shared technological affordances of cybersecurity technologies, it is also due to the economic motivations of defence companies and specialist surveillance suppliers. These companies both acquired many cybersecurity companies and integrated others into their supply chains and products, reinforcing technological overlaps with institutional and individual links. This entanglement is crucial to my argument, as it allowed these surveillance suppliers to draw on wider values to manipulate organisational, national security, and rights-based conceptions of cybersecurity.

8.2 Assimilating human rights values

This section argues that private sector surveillance suppliers assimilated human rights values flexibly in what I call the moral manoeuvre of manipulation. Many scholars have argued that commercial security providers can define the scope of security issues themselves, aside from their more obvious economic and operational influence.[551] However, this scholarship has rarely overlapped with work on the values of private companies more widely, despite the international legal view that there is a "strong moral case" that companies are obliged to protect human rights.[552] Supporting this view, the UN's 2011 Guiding Principles on Business and Human Rights, clarified that businesses should both avoid contributing to human rights violations and prevent those that are "directly linked" to their operations, even if they did not contribute to them.[553]

---

[550] Wikileaks, 'Hacking Team Email-ID 574463', 6 May 2011, https://perma.cc/7BME-8MJU; Shane Harris, 'U.S. Hired Dictators' Favorite Hackers', *The Daily Beast*, 7 July 2015, https://perma.cc/2X8H-97YQ.
[551] Anna Leander, 'The Power to Construct International Security: On the Significance of Private Military Companies', *Millennium* 33, no. 3 (1 June 2005): 803–25; Rita Abrahamsen and Anna Leander, eds., *Routledge Handbook of Private Security Studies* (London; New York: Routledge, 2015); Abrahamsen and Williams, *Security Beyond the State*.
[552] Philip Alston, ed., *Non-State Actors and Human Rights* (Oxford; New York: Oxford University Press, 2005), p.23.
[553] United Nations, 'Guiding Principles on Business and Human Rights' (HR/PUB/11/04, 2011).

The relationship of private companies to human rights has been applied specifically to the internet and digital technologies. Notably, Dann and Haddow created a typology of the excuses for human rights violations given by technology companies when cooperating with repressive governments. Dann and Haddow's concept of 'excuses' occupies similar terrain to the moral manoeuvre of manipulation detailed here, but lacks my emphasis on the way in which companies retain the flexibility both to adhere to and circumvent human rights constraints.[554] Separately, Deibert, Flyverbom and Matten have argued that technology companies have new responsibilities regarding surveillance and data management.[555] This section can be seen as an interrogation of those responsibilities in the specific case of surveillance suppliers to national governments. This section first considers the example of Hacking Team, and then widens the scope to other companies treated in the previous section.

8.2.1 Hacking Team

Hacking Team (HT) has a stronger connection with the region studied by this thesis than most other surveillance suppliers, as they are part-owned by a Saudi Arabian investor. In February 2018, the technology website Vice reported that a Cyprus-based company called Tablem Limited, reportedly associated with several individuals in the Saudi government, specifically the Ministry of Communications and Information Technology, were likely behind a large purchase of HT shares.[556] According to this report, David Vincenzetti, the founder and CEO of Hacking Team, avoided commenting on the purchase, saying that "the Saudi government is opaque even for me… I don't have visibility in the role nor the activities of this person in Saudi [Arabia]."[557] However, a former HT employee put forward a different view, saying that "there's the Saudi government behind it, the

[554] Gary Elijah Dann and Neil Haddow, 'Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet', *Journal of Business Ethics* 79, no. 3 (1 May 2008): 219–34.
[555] Mikkel Flyverbom, Ronald Deibert, and Dirk Matten, 'The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business', *Business & Society*, 26 August 2017.
[556] Lorenzo Franceschi-Bicchierai, 'Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia', Motherboard, 31 January 2018, https://perma.cc/ZR94-TANK.
[557] Franceschi-Bicchierai.

money comes from them… They [HT] were on the brink of bankruptcy, and that's when David sold his soul to the Saudis to save the company."[558] On top of the note of Faustian moral bankruptcy implied by working with the Saudi government, this employee suggests that HT thus has much greater dependency on this region, and Saudi Arabia in particular, than many other companies. As noted in Chapter 6, its software has been identified in Egypt and all GCC states other than Kuwait and Qatar.

HT themselves were hacked in 2015, after which many internal documents and emails were leaked online. These documents provide a unique insight into the manipulation of different values and provide another reason to focus on HT in detail. Before I examine the documents themselves, the values motivating the hack itself deserve brief consideration. An apparently authentic account of how HT systems were compromised was published anonymously under the pseudonym Phineas Fisher, who finished the account as follows:

> Hacking guides often end with a disclaimer: this information is for educational purposes only, be an ethical hacker, don't attack systems you don't have permission to, etc. I'll say the same, but with a more rebellious conception of "ethical" hacking. Leaking documents, expropriating money from banks, and working to secure the computers of ordinary people is ethical hacking. However, most people that call themselves "ethical hackers" just work to secure those who pay their high consulting fees, who are often those most deserving to be hacked.[559]

This quotation serves as a reminder that as well as the values considered in this thesis – whether organisational or rights-based – there is another, more anarchic, cluster of values in cybersecurity that is not within the scope of this thesis.

I use the documents leaked by Phineas Fisher to examine Hacking Team's internal communications over a short period, between November 2013 and April 2015. This period stretches from the amendment to the Wassenaar Arrangement itself, in December 2013, to the implementation of the amendment in the EU, including Italy, where HT are based, in early 2015. Although, as I argue below, the Wassenaar amendment does not simply act as a norm socialising HT into compliance, their manipulation of values is most clearly expressed in their discussions in this period. The relevant

[558] Franceschi-Bicchierai.
[559] Phineas Fisher, 'Hack Back! A DIY Guide', April 2016, https://perma.cc/QZE6-55R5.

internal debates are centred on publicity and public image: either articles about HT to which they react or provide comment, or discussions around public statements, customer policies, and similar events. These discussions are important because they contrast public statements about values with both the strategic reasons behind those statements and the values expressed by HT in private.

The first relevant email exchange was in November 2013, at the time of the Wassenaar amendment, when Hacking Team discussed how to describe the countries to which they would not sell their surveillance software.[560] The first suggestion was that "we do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN." This provoked substantial discussion, as one reply stated that "I really don't like "blacklisted"", and another suggested it is too vague. A further reply reinforced this point, saying that "I am not sure what we look at when we determine whether or not a country is someone we don't want to do business with". In the end, the alternatives 'sanctioned' and 'embargoed' were rejected, as "blacklisted is more general, it is better".

This early discussion illustrates two points. First, HT did not internally adopt a value-based justification for restricting sales of their software, instead relying on internationally agreed criteria. Second, and in contrast to the view of international export restrictions as clear 'norms' to follow, they decided on a description of these external criteria as 'blacklisting 'precisely because it was vague (or 'general'), despite dissenting voices. This vagueness allows room for manoeuvre, as HT made clear in subsequent discussions.

The second email chain was a few months later, in March 2014, after inquiries by Human Rights Watch about HT software.[561] Their Customer Policy at the time stated that:

> We expect our clients to behave responsibly and within the law as it applies to them… In HT contracts, we require customers to abide by applicable law. We reserve the right in our contracts to suspend support for our software if we find terms of our contracts are violated. If we suspend support for HT technology, the product soon becomes useless.[562]

[560] Wikileaks, 'Hacking Team Email-ID 166153', 5 November 2013, https://perma.cc/HWK7-R897.
[561] Wikileaks, 'Hacking Team Email-ID 72106', 26 March 2014, https://perma.cc/9JGB-LATM.
[562] Wikileaks.

HT emphasised in this email chain that clients are constrained by "the law as it applies to them". As seen in the previous chapter, in Egypt and the Gulf states this includes expansive definitions of national security and cybercrime, with few constraints. Here, HT initially seemed to adopt the identity of a 'mere' technology provider rather than law enforcement partner, based on the premise that government 'clients' operate the software rather than HT themselves.

However, this apparent lack of responsibility is called into question by the last clause of the paragraph above (elsewhere phrased as 'the product becomes vulnerable to detection and therefore useless"). Claims elsewhere that "Hacking Team installs it, releases the updates, but can't in any way know what it's used for" are contradicted by technical analysis that indicates they have detailed control over their technologies once sold to customers.[563] In internal discussions over their Customer Policy, their route out of this dilemma was as follows:

> Of course we cannot say we have direct control over installations of our software, but with this phrasing we reserve to exert control, yet we don't specify exactly how the software is made ineffective. I'm using "advances in computer technology" as the motivation since it's generic enough to not let them point to a specific measure. In this way, we keep us responsible to a reasonable extent, but we prevent external verification.[564]

This is a crucial quotation for my argument. HT here manipulated the public description of their technology to give them flexibility in choosing when to restrict sales of their software. They chose the specific phrase 'advances in computer technology' because it shows that they *can* prevent human rights violations (i.e. appear to agree with the NGOs calling for controls on this software), but simultaneously can also 'prevent external verification', meaning that they can choose not to investigate situations that NGOs would consider abuses. HT here altered not just values but also technical claims surrounding those values to achieve their strategic aim of surveillance sales.

A subsequent email chain, in May 2014, took this alteration of values further. In an internal discussion concerning an article about HT and the Wassenaar amendment in Slate magazine, HT stated the following:

---

[563] Lorenzo Franceschi-Bicchierai, 'Leaked Emails Show Hacking Team Lied to Its "Rascal" Customers', Motherboard, 14 July 2015, https://perma.cc/9VUG-Z2FJ.
[564] Wikileaks, 'Hacking Team Email-ID 72106'.

> We should definitely present ourselves as an active and interested part into the regulatory discussion… Any type of regulation will be ineffective at stopping human rights abuses by itself and regulation should also take into consideration that criminal investigation and intelligence operations showed a clear needs for this type of technology… The real issue is not the technology, but the behaviour of oppressive governments. Activists should direct their efforts toward the problem states.[565]

This quotation shows that HT agreed internally to portray themselves as *contributors* to the Wassenaar amendment, rather than its targets. This quotation incorporates both national security and human rights values: the former by referring to the 'clear needs' of governments and the latter by using the language of NGOs around 'oppressive governments' and 'problem states'. Furthermore, by suggesting that regulation will be 'ineffective', HT implied that they care more about human rights violations than those who seek to regulate them. Here they both distanced themselves as technology providers from association with human rights violations *and* signalled their affinity with the values of NGOs, all with the aim of preventing regulation from interfering with sales.

This manufactured affinity with the value orientation of human rights NGOs also enabled HT to experiment with a victim narrative. In an email chain in June 2014, directly following a report by Citizen Lab on HT cited in Chapter 6, HT integrated now-familiar themes of distance from investigations and the assimilation of rights values into a claim that HT *themselves* were the vulnerable party, rather than individual citizens, states or any other standard referent for cybersecurity discourses:

> Hacking Team is in the same position most Security Agencies are: very good at (providing the necessary tools for) protecting a Country from a variety of menaces (e.g., serious organised crime, drug cartels, insurgents) but very bad at protecting themselves. As you know, we do NOT actually perform any digital investigation: we just provide Police forces and Security Agencies with our technology… But activists like Citizens Lab equate HT software with human rights abuses. In truth, Citizen Lab's complaint is not with HT but with repressive regimes, and so be it. But to attack a private company because you don't like the actions of certain governments (like Saudi) that you cannot attack (because it's harder) is reprehensible.[566]

In this quotation HT repeated their assimilation of both a perspective of national security, protecting states from 'menaces', as well as acknowledging the relevance of 'human rights abuses'.

[565] Wikileaks, 'Hacking Team Email-ID 174340', 26 May 2014, https://perma.cc/SR6E-BVM4.
[566] Wikileaks, 'Hacking Team Email-ID 171363', 30 June 2014, https://perma.cc/EW6Y-8AT6.

Furthermore, in a separate email chain in August 2014 a HT employee went further than the claim above that Citizen Lab are 'reprehensible', suggesting that even other cybersecurity companies could also be viewed as threats: "Because our product is used to fight crime and terrorism, the antiviruses keep at large bandits and criminals. The antivirus, from the lea [law enforcement agency] point of view, is a partner in crime."[567] Although this suggestion was rejected by others, it highlights how far HT conducted calculated internal discussions about the manipulation of values that are not manifest in their public statements.

These discussions led to a more sophisticated public image, demonstrated by an email chain in August 2014, which answered questions posed by a Washington Post reporter. Here, in the passage with which I began this chapter, HT honed earlier claims of technologically-enabled distance from human rights violations within a frame of 'misuse':

> We thoroughly vet potential clients before any sale. A review board has a veto over sales that pose a risk of misuse. If we learn of possible misuse after a sale, we investigate and take action that may include suspending support for the suspect system. We provide within the system checks that permit supervisors to know how and when the system has been deployed to track activity of a subject. This cannot be disabled… We share with Citizen Lab a concern for human rights throughout the world, but we share with law enforcement authorities around the world a concern that the Internet and mobile technologies can be used for criminal activities as well as for good… we believe that HT is the ethical as well as the technological leader in our industry. [568]

The appearance of the concept of 'misuse' is central to the manipulation of values by surveillance suppliers and will be examined further in the following section. Here, I emphasise only that this quotation combines the various forms of manipulation detailed so far, including technological facilities to monitor surveillance equipment after it is sold, the assimilation of both human rights and national security values, and the overall claim that HT is an 'ethical leader'.

Despite ample evidence of manipulation, there are some indications from these leaked emails that norm theories of socialisation accurately identify a source of pressure on surveillance suppliers, even if they misdiagnose the effects of this pressure. For example, after Citizen Lab's report about an application targeted at the Qatif region of Saudi Arabia that downloaded HT software,

[567] Wikileaks, 'Hacking Team Email-ID 120169', 22 August 2014, https://perma.cc/GQ92-FFQC.
[568] Wikileaks, 'Hacking Team Email-ID 149888'.

one participant said that "Since we say we investigate cases like this, that we should do so in the case of these reports regarding Saudi".[569] This indicates that international norms exert *some* pressure on actors to conform. However, given that HT were later bought out by a Saudi investor, I infer that HT did not stop providing software to Saudi Arabia in this case and that this pressure was limited.

Another indication that norm-based theories of socialisation are partly accurate is from an email chain in March 2015, following negative publicity from the association of their software with human rights violations in Ethiopia. In this discussion, a Hacking Team employee stated that "the only right move right now is stop supporting the customer forever. so they cannot embarrass us in the future again. so we can re-assert that from jan 2015 we are wassenar compliant".[570] This employee not only recognised the importance of *asserting* compliance but appeared prepared to follow this through by dismissing their customer. For this employee, this was the 'right move' for social reasons (embarrassment), indicating the pressure exerted by international norms. Nonetheless, media reports indicate that HT continued to sell their software to Ethiopia after a brief suspension in March 2015, demonstrating the limits of this pressure.[571]

Crucially, even in this case HT still sought to exploit human rights values for commercial benefit. Another comment in the same email chain stated that "this customer is not worth the problems they are causing… it wouldn't hurt for the activists or frankly other clients to know [that they were cut off]". This provides a rare insight into the multidimensional strategic decisions taken by Hacking Team, as they not only look to use human rights language against their critics, but also against *other clients*, seeking to ensure other clients help them avoid such negative publicity and maintain sales.

In sum, HT manipulated both human rights and national security values in navigating a rapidly shifting environment around the Wassenaar amendment. This was *not* a socialisation process: even though internal discussions reveal that international norms exerted some pressure on HT employees, this pressure was limited and avoided. Instead, Hacking Team deliberately built in

[569] Wikileaks, 'Hacking Team Email-ID 164478', 28 June 2014, https://perma.cc/UX4G-NNQH.
[570] Wikileaks, 'Hacking Team Email-ID 49934', 7 March 2015, https://perma.cc/RR6Y-N2R7.
[571] John Leyden, 'Hacking Team Mulled Stopping Ethiopia Sales – Because of Idiot g-Men', The Register, 17 August 2015, https://perma.cc/RP3J-ULFF.

flexibility to their commitment to both sets of values and improvised both proactive and reactive strategies to reinterpret these values in ways which achieve their overall goal: sales of surveillance software.

8.2.2 Other companies

The investigation of Hacking Team above has several limitations, not least of which is representativeness. Hacking Team is only one company in a whole ecosystem of surveillance suppliers. This section extends the investigation above to other surveillance suppliers, albeit without the insights gained from internal discussions.

Some surveillance suppliers exploited the dual-use possibilities of the DPI-based surveillance systems discussed in Chapter 6. A report by Al-Jazeera in 2017 detailed conversations an undercover reporter conducted with various surveillance suppliers, including another Italian company, IPS, which provides DPI-based monitoring systems. The sales manager for IPS reportedly claimed that he could disguise surveillance systems as "software analytics for statistics for traffic congestion, because although these surveillance systems were "subject to export restriction… this is something we can manage."[572] These companies also claimed they were merely technology providers, like Hacking Team. An employee of another company interviewed by Al-Jazeera, AREA, was reportedly "told the company wasn't responsible for how the system would be used", after surveillance sales to Syria.[573]

Other companies, such as Procera Networks (later changed to Sandvine), include filtering and censorship within their overall 'traffic management' services. However, in a 2016 brochure they caution their customers that "blocking… requires local dedicated personnel to perform well. Procera can provide these resident engineering services."[574] Many other surveillance suppliers also provided

[572] Al-Jazeera Investigative Unit, 'How the "Dual-Use" Ruse Is Employed to Sell Spyware', *Al-Jazeera*, 10 April 2017, https://perma.cc/SQ6E-76ZY.
[573] Al-Jazeera Investigative Unit, 'Spy Merchants: Spying on Dissent through Illegal Means', *Al-Jazeera*, 10 April 2017, https://perma.cc/2CNY-EQR2.
[574] Procera Networks, 'Use Cases', 2016, https://perma.cc/X8XE-SJ5Z.

continued support of their systems after purchase. Documents leaked from FinFisher in 2014 suggest that security agencies in Qatar and Bahrain encountered technical problems, which they claimed affected their investigations.[575] A report on Amesys, a French surveillance supplier to Egypt mentioned in Chapter 6, claimed that "every 45 days, technicians from Dubai or Paris visit the various sites in order to train employees and to finalise the implementation of the system."[576] These relationships and recurring technical problems, also surfacing in leaked documents from Hacking Team, highlight the close relationships all surveillance companies have with their customers.[577]

Some reports indicate an approach to surveillance sales that sees human rights values as irrelevant. For example, the Amesys report above included an interview with an anonymous French surveillance specialist who stated that:

> Of course the French services sub-contract technical intelligence. It's either that or handing control to the Chinese or the Israelis. We aren't Carebears. We tell ourselves we are doing it in the interests of our country. In any case, all the countries are equipping themselves, whether its through us or elsewhere.[578]

However, this position is never taken publicly (compare the private statement by Hacking Team's CEO in the quotation at the start of this chapter). Instead, other companies publicly adopted human rights values in a similar way to Hacking Team. NSO Group claims to have "an ethics committee made up of employees and external counsel [which] vets potential customers based on human rights rankings set by the World Bank and other global bodies".[579] The workings of this ethics committee are not publicly available, although a New York Times report on NSO Group claimed that they had never been denied an export licence.[580]

Sandvine is another company with a clear public adoption of human rights values. Following Citizen Lab's discovery of Sandvine software in Egypt and Turkey in 2018, Sandvine wrote to

[575] Wikileaks, 'Finfisher - Customers', 15 September 2014, Spy Files 4, https://perma.cc/MVB9-8VDC.
[576] Tesquet, 'Amesys'.
[577] Wikileaks, 'Hacking Team Email-ID 432563', 30 December 2013, https://perma.cc/9PGK-CAMD.
[578] Tesquet, 'Amesys'.
[579] Nicole Perlroth, 'How Spy Tech Firms Let Governments See Everything on a Smartphone', *The New York Times*, 2 September 2016, https://perma.cc/3STM-RR9U.
[580] Thomas Fox-Brewster, 'Everything We Know About NSO Group: The Professional Spies Who Hacked IPhones With A Single Text', Forbes, 25 August 2016, https://perma.cc/G3ZG-CL5Y.

Citizen Lab explaining their ethical and moral commitments. While in this case I do not have access to the debates behind these letters, their content is similar to publicity statements by Hacking Team:

> A key part of [Sandvine's] innovation process is to ensure that we do not lose sight of the ethical impact of our technology on human rights, freedom of speech, and privacy. Sandvine has taken the approach on regulating access to the components of our solutions that could be used to infringe on any of these. The usage of our regulatory compliance solutions are controlled by… software licenses that are required for any components that could conceivably be used to violate human rights, freedom of speech, and privacy.[581]

Here Sandvine assimilated the language of human rights in a sophisticated way. Sandvine's commitments included a Business Ethics Committee that uses the "World Bank Index" to make decisions over certain sales, in the same manner as Hacking Team's 'review board' and NSO Group's 'ethics committee'. This is a common element of the corporate structure of surveillance suppliers, and it deserves close scrutiny. Both NSO Group and Sandvine claim to use World Bank indicators to judge the risk of human rights violations associated with their technologies. However, as they do not specify the exact metrics, nor how risks are calculated using these metrics, this technique forms part of the moral manoeuvre of manipulation: assimilating human rights values into public statements, while retaining sufficient flexibility to continue sales in general *and* restrict certain sales if necessary for reputational reasons.

BAE Systems, whose software was the subject of a BBC report in 2017,[582] justified their sales to the Gulf states by claiming that "our technology plays a crucial role in enabling the UK and its allies to combat the threat of international terrorism, supporting law enforcement and helping to keep the public safe, both in the UK and abroad".[583] BAE also adopted the frame of misuse used by Hacking Team, in a passage worth quoting in full:

> The BBC also acknowledges there is no evidence that these BAE Systems products have been misused. BAE Systems is committed to operating ethically and responsibly. We have robust policies and procedures in place to ensure that our international exports to overseas governments are all fully compliant with international export regulations as

[581] Marczak et al., 'Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?'
[582] BBC, "How BAE Sold Cyber-Surveillance Tools to Arab States," *BBC News*, June 15, 2017, https://perma.cc/75ZM-NXYD
[583] Jason Murdock, 'BAE Systems "sold Powerful Spy Technology to Repressive Regimes" across Middle East', International Business Times, 15 June 2017, https://perma.cc/BT7R-QQFD.

> well as our own strict criteria to evaluate every potential contract. If we believe there may be a risk of misuse, we will refuse the business.[584]

We see here that these surveillance companies use the alignment discussed in Chapter 6 to their full advantage. Because NGOs aligned human rights values with dominant values in cybersecurity to promote human rights as a referent object for security, surveillance companies were able to respond by mimicking the fine line between legitimate cybersecurity technologies and illegitimate uses drawn by opponents to the Wassenaar amendment. Here, the legitimate use is not protection against cybersecurity threats but more broadly 'supporting law enforcement and keeping the public safe'. Nonetheless, the logic is identical, and through the concept of 'misuse' this logic transforms an opposition between very different sets of values into a finely balanced risk calculation between two similar uses.

Although this discussion has so far indicated that many of the elements of the Hacking Team documents are replicated elsewhere in the surveillance ecosystem, it has so far remained at the level of public statements. To dig behind these statements, I draw on presentations from a workshop held at the University of Oxford under Chatham House rules in March 2018. Although I cannot name the participants due to the Chatham House rule, presentations confirmed details of the above discussion.

One participant confirmed the requirement for constant support of surveillance technologies, saying that "one of the constraints is that the whole product would fall apart if our engineers aren't on site for 48hours, so it wouldn't work." They also agreed that there was no public alternative to their assimilation of human rights:

> We have branded ourselves as a company that protects [human rights values]. Other companies will not get the same scrutiny as we do. With surveillance and Syria, they comply with all laws and most didn't take any flak because they didn't make any claims otherwise.

This company also recognised the potential effects of their technologies on state stability overall, rather than being associated with specific human rights violations. In the following quotation a presenter put the question in terms of the desirability of autocratic regimes:

[584] Murdock.

> How do we draw red lines? In the example of workers that are unfairly treated to build stadiums, we are protecting stadiums and helping [certain states] succeed. Three steps down the road we are responsible, should that factor into our decision?

This presenter also revealed two moral dimensions to their decisions that were not identified in either the Hacking Team emails or the discussion of other companies above. One was the question of altering the technologies themselves without alerting their customer.

> For example, the telecoms system is owned by the government. We are asked to build a search tool, we said that's an easy way to do fishing expedition [i.e. search for any phone number and related content], this really sucks. Let's build it so you have to enter a phone number, but we didn't tell the customer this is what we were doing, we said it was for performance reasons.

While Hacking Team used technical claims to distance themselves from human rights violations, here the presenter claimed to use benign reasons of 'performance' to prevent such violations actively at the design stage rather than after accusations of complicity. The alternative, for this presenter, was to be more open about their values with the customer. However, the presenter recognised that this route meant that human rights values would be more likely to be violated without their knowledge: "if we tell our customers all this stuff, do we give them a road map to lie to us? Are we making it easier for them not to disclose what the system is being used for?" The manipulation of values is thus a strategic operation at several levels, not only regarding norm proponents such as NGOs, but also including conflict and lack of trust between surveillance suppliers and their client governments. Finally, a presenter took this lack of trust further to shed a different light on the misuse procedures publicly adopted by several surveillance companies including Hacking Team, NSO Group, Sandvine and BAE Systems. In a fascinating rumination, they said:

> Can we be even sneakier? We have access to audit logs… For example, there is a country arresting people due to comments on social media, we were worried about this and we knew the names of people that were being arrested [so we checked whether they were in our audit logs]. We are glad it wasn't being used for that [i.e. this company's tools used to assist the arrests] but should we have done that without telling customer? Have we already given them enough notice?

The response to suspected misuse here was not to refer to an ethics committee and question the overall commercial relationship between the surveillance supplier and the client government. Instead, this presenter claimed that they used audit logs to investigate - without the client's

knowledge - whether their client was violating human rights by arresting social media users. This quotation underscores the complexity of both the moral and technical environments in which these surveillance suppliers operate. There is no clear sense of what 'compliance' means, whether in relation to regulations such as the Wassenaar Arrangement or policies of abuse and misuse created by the companies themselves. Instead, engineers implementing surveillance systems *on the ground* creatively improvise solutions that renegotiate both the instantiation of abstract values in specific circumstances, and the technological capabilities of their surveillance systems.

In sum, norms theories of socialisation or compliance do not adequately capture the way these companies manipulate both human rights values and other values such as national security in combination with precise technical claims about both the design and operation of their software. In contrast, the moral manoeuvre of manipulation assimilates a range of values but remains agnostic regarding normative commitment to any one value or cluster of values. Instead, manipulation builds in flexibility with the overarching goal of maintaining sales of surveillance equipment.

8.3 Exporting states

This section examines the moral manoeuvre of manipulation as performed by exporting states rather than private sector surveillance suppliers. Although their actions are different in many ways, they have two key similarities. First, they are motivated by an economic goal: increased exports and consequent capital flows into their economies. Second, they are centrally concerned at retaining flexibility, both restricting sales and enabling them where it suits their trade goals. I first provide a brief overview of links between Egypt and the Gulf states on one hand, and the UK and US on the other hand, in defence, intelligence and cybersecurity. I then examine the UK's export policy in detail as a key example of manipulation.

8.3.1 Defence, intelligence and cybersecurity

The governments of Egypt and the Gulf states have strong defence relationships with many states, especially the US and UK. Both UK and US maintain a large military presence in the Gulf, with the GCC split implying only that defence agreements be secured with both sides to maintain impartiality. While both the UK and US are key players in the Gulf, the Egyptian defence sector is primarily supported by the US. Although the Egyptian military makes occasional deals with other countries for both genuine capability and foreign policy purposes, its prime strategic partner remains the US. Following the cancellation of Egypt's $7.1 billion military debt to the US after the Gulf War in 1991, the US has continued to supply military finance as aid, and Egypt receives around 20% of all total Foreign Military Financing for the US globally.[585]

The US and the UK occupy different positions in the global arms market. As Buzan and Herring note, the US is a top tier producer *and* consumer, and so can restrict exports without significant effect on its industries.[586] The UK is a middle-tier producer and so has more pressure on maintaining exports. Nonetheless, it claims to have "one of the most robust export regimes in the world", and was a key proponent of both the 2014 Arms Trade Treaty and the 2013 amendment to the Wassenaar Arrangement.[587] The UK strategy is encapsulated by the then-defence secretary Liam Fox's comment that "I want to make sure the United Kingdom – within the limits that we set ourselves ethically on defence exports – is getting a healthy slice of that [market]".[588]

Military links between this region and the US and UK also cover intelligence cooperation, with a long imperial legacy. As intelligence historian Richard Aldrich observed, "British dominance of international telecommunications networks meant that many of the world's messages travelled over British cables at some point [and] private companies such as Standard Cable & Wireless Ltd

[585] Project on Middle East Democracy, 'US Military Assistance to Egypt: Separating Fact from Fiction' (POMED, January 2018).
[586] Barry Buzan and Eric Herring, *The Arms Dynamic in World Politics* (Boulder: Lynne Rienner Publishers, 1998), pp.75-83.
[587] BBC, 'How BAE Sold Cyber-Surveillance Tools to Arab States'.
[588] Staff Report, 'Liam Fox Defends Mideast Arms Sales', The Independent, 22 February 2011, https://perma.cc/5Y7E-QUV9.

were almost an integral part" of intelligence collection from these cables throughout the twentieth century.[589] This was likely the case in the Gulf states: in Saudi Arabia, Cable & Wireless won several military contracts following King Fahd's modernisation in 1970, and also owned a controlling stake in the Bahrain and UAE telecoms operators founded at a similar time.[590]

The US and UK are also the two founding members of the Five Eyes intelligence alliance (with New Zealand, Australia, and Canada), which has extensive surveillance capabilities. As part of its contribution to this alliance, the UK has had a satellite interception station in Seeb, on the coast of Oman, since at least 1990, and in 2009 this station was upgraded to provide access to the large number of undersea internet cables coming ashore there.[591] Documents released by Edward Snowden demonstrate the importance the US National Security Agency (NSA) attaches to collection from undersea cables, and the role of the UK in enabling their access.[592] Leaked documents in 2017 indicated that the US National Security Agency (NSA) covertly obtained persistent access to a vast quantity of financial information from UAE banking services provider Eastnets,[593] as well as maintaining a key data collection and analysis centre in Egypt.[594]

Mirroring earlier imperial relationships, this activity is not without benefit for some in the relevant governments: Saudi Arabia and the UAE are approved 'Third Parties', able to access some US signals intelligence.[595] This relationship also covers the offensive cyber capabilities noted in the first section of this chapter. For example, leaked emails from the UAE Ambassador to the US included a "discussion of possible U.S./UAE policies to positively impact Iranian internal situation",

[589] Richard Aldrich, *GCHQ* (London: HarperPress, 2010), p.17.
[590] Department for Trade and Industry, *Telecommunications Related Opportunities for UK Companies in the Kingdom of Saudi Arabia* (London: UK Government, 1988), pp.106-107.
[591] Duncan Campbell, 'REVEALED: GCHQ's BEYOND TOP SECRET Middle Eastern INTERNET SPY BASE', The Register, 2014, https://perma.cc/K3YU-66XZ.
[592] Frederik Obermaier et al., 'Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts', Sueddeutsche Zeitung, 25 November 2014, https://perma.cc/39JK-Z39V.
[593] Clare Baldwin, 'Hackers Release Files Indicating NSA Monitored Global Bank Transfers', *Reuters*, 15 April 2017, https://perma.cc/V2R2-N5KA.
[594] Elias Groll, 'Meet the NSA's New Data Centers: Russia, China, and Venezuela – Foreign Policy', Foreign Policy, 31 July 2013, https://perma.cc/YLD6-LXMF.
[595] Duncan Campbell, 'NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET', The Register, 5 June 2014, https://perma.cc/PR4D-25NC.

focusing on "political, economic, military, intelligence, and cyber tools… to contain and defeat Iranian aggression."[596]

However, some interviews indicate that this strategic alliance is not an equal partnership, as the UK motto of "Gulf security is our security" might suggest.[597] As one UK interviewee explained, "we see these countries as our frontline, it's the same strategy as terrorism. These countries are our cyber Forward Operating Bases" (I-49). The suggestion made by this interviewee, that the GCC countries are merely outposts – or the 'frontline' - of British power, has strong colonial echoes, implying both that securing overseas territory is conceptually coherent in the transnational and fluid domain of cyberspace, *and* that the possession of this overseas territory, as a British base echoing the old stone castles dotted along the Gulf coastline, is a desirable strategy.

How does this intelligence partnership feed into the surveillance ecosystem considered so far in this chapter? Intelligence departments in the UK and US are key aspects of their domestic cybersecurity governance structures. When these departments train their regional counterparts in cybersecurity, as the UK Prime Minister Teresa May stated in a 2016 launch of the UK's Gulf Strategy, this builds both a similarity of approach and a significant degree of trust between them.[598] Leaks of this intelligence capability can undermine trust with the region, as one non-UK European interviewee noted regarding the Snowden leaks: "the US and UK screwed up because they opened Pandora's box, and against their own allies" (I-36).

Despite this, an underestimated aspect of the intelligence impact on cybersecurity is that it is a very effective commercial advertisement. As a UK interviewee stated: "The Middle East rates the UK as one of the best countries to source cyber capability. It's a secondary effect of the Snowden revelations… Snowden kicked us in the nuts, but people had no idea what GCHQ and NSA were doing before then." (I-47). Without space to delve into the underlying national masculinities on display, this quotation illustrates the marketing effect of publicly revealed surveillance capabilities,

[596] Zaid Jilani and Ryan Grim, 'Hacked Emails Show Top UAE Diplomat Coordinating With Pro-Israel Think Tank Against Iran', The Intercept, 3 June 2017, https://perma.cc/JQ5H-FNPW.
[597] Teresa May, 'Prime Minister's Speech to the Gulf Co-Operation Council 2016' (UK Government, 2016), https://perma.cc/PFL9-73YR.
[598] May.

providing a boost to the private sector surveillance suppliers and defence companies examined so far in this chapter. In sum, Egypt and the Gulf states have strong relationships in defence and intelligence with the UK and US, and the latter have extensive financial incentives for facilitating the sale of surveillance equipment to the region.

8.3.2 UK export policy

This section argues that, like the private sector surveillance suppliers considered earlier in this chapter, the UK also manipulates values and technical claims to maintain sales of surveillance software. As an exporting state that is both a norm entrepreneur in the regulation of arms exports *and* a market leader in cybersecurity and surveillance technologies, the UK occupies a complex position not recognised by standard accounts of norm socialisation and compliance, as in their view, the UK would be a *socialising* actor rather than an actor manipulating pressures of socialisation.

In the UK, the Wassenaar list of dual-use technologies feeds into the UK's 'Consolidated List', which includes both technologies from various international treaties and those separately deemed worthy of export control by the UK government.[599] This process is mediated by the EU, as follows. First, the Wassenaar committee must approve additions to the list. Then, as the Wassenaar Arrangement is applicable in the EU through a 2009 European Council regulation, the European Commission must update its own dual-use list, which it did in October 2014.[600] Only then must individual member states incorporate this list into their domestic legislation (which varies throughout the EU, and which in the UK is the Export Control Act 2002). The UK included intrusion and surveillance software in its export control list in January 2015.[601]

It is worth noting that, as well as the general Wassenaar amendment, the EU made several specific statements on the sale of surveillance technologies to Egypt following the 2013 coup. First,

[599] Export Control Organisation, 'Consolidated List of Strategic Military and Dual-Use Items That Require Export Authorisation' (UK Government, 13 July 2017).
[600] EU Commission, 'Commission Delegated Regulation (EU) No 1382/2014', 22 October 2014, https://perma.cc/R7DP-CV7G.
[601] 'Consolidated List of Strategic Military and Dual-Use Items That Require Export Authorisation - GOV.UK', 6 January 2015, https://perma.cc/459D-2DA6.

the Foreign Affairs Council made a statement on 21 August 2013 calling on EU members "to suspend licences for the export to Egypt of any equipment used for internal repression".[602] Then, on 15 January 2015, the EU Parliament "called for an EU-wide ban on the export to Egypt of intrusion and surveillance technologies which could be used to spy on and repress citizens."[603] The UK, at the time of writing, also uses these statements and rulings to make export decisions.

In contrast to the UK's image as a 'steward state' of human rights, in this sector the UK government avoided export decisions based on human rights values wherever possible.[604] A key question for export policy in the UK – and, incidentally, the question that most animated those in the cybersecurity department of DIT in interviews – is how to judge whether a company is based in the UK. BAE Systems has a separate US arm, and has acquired business from many other countries, including Danish company ETI. The BBC investigation into these sales quoted an email from the UK export authorities to their Danish counterparts stating they would have refused this export due to national security rather than human rights concerns. In this case, not only did BAE's multinational reach enable them to avoid stricter export controls, even between EU countries who are all obliged to implement EU human rights clauses stemming from the Wassenaar Arrangement, but the UK government chose to cite national security rather than human rights reasons to try and prevent it. The UK therefore did not act simply as a norm entrepreneur for human rights in relation to surveillance exports in this case.

This avoidance of explicit human rights values can also be seen in UK government communications to the cybersecurity industry. TechUK, a government-business liaison body, issued guidance in November 2014, just before export controls came into force, called "Assessing cybersecurity export risks".[605] This document used many of the examples cited in Chapter 6 to demonstrate human rights concerns, and was drafted by the UN-supported Institute for Human

[602] European Parliament, 'Motion for a Resolution on Egypt (2013/2820)', 10 September 2013, https://perma.cc/5ZT7-4DQY.
[603] European Parliament, 'European Parliament Resolution on the Situation in Egypt (2014/3017)', 15 January 2015, https://perma.cc/SJ8S-RGXY.
[604] The term is from Emilie M. Hafner-Burton, *Making Human Rights a Reality* (Princeton, New Jersey: Princeton University Press, 2013).
[605] TechUK, 'Assessing Cyber-Security Export Risks' (UK Government, 19 November 2014).

Rights and Business. However, this guidance avoided explicitly ethical justifications for action: while it still addressed the risk of human rights violations, companies were encouraged to engage for "reputational risk" and "long term profitability". The risk here was portrayed as economic, with human rights as a reputational issue. In this case, even states that *promoted* the Wassenaar amendment did not seek to communicate the values behind their decision to companies, casting them as purely economically motivated actors.

This guidance also contributed to confusion over the term 'cybersecurity' by firmly including all technologies examined above in this bracket. It described surveillance technologies as 'specially designed for offensive cybersecurity purposes", a stretched interpretation of 'cybersecurity' even compared to many of the companies' own descriptions, and one which contradicts the Wassenaar Arrangement's description of its mass market exemption, examined in Chapter 6, as a 'cybersecurity exemption'. The UK here reinterpreted cybersecurity to such an extent that it offered a new definition of the issue area itself.

Like private sector surveillance suppliers, the UK also manipulated calculations of risk and misuse to maintain surveillance sales. To export controlled items from the UK a company must request an export licence from the Export Control Organisation (ECO), which is part of the Department of International Trade (DIT, formerly the Department of Business, Innovation, and Skills). Export licences may be general, open or specific; respectively allowing export by any company of a whole class of items to a specified list of countries (e.g. cryptographic equipment), allowing one company to export a class of items to a specified list of countries, or allowing a particular contract.[606] An open licence was granted in October 2015 for a company to export targeted surveillance software to eleven countries including Egypt, Qatar, Saudi Arabia, and the UAE, and a specific licence was granted for a surveillance contract worth £6.5 million to the UAE in July 2015 (the data released by the ECO does not identify the company).[607]

[606] Export Control Organisation, 'Open General Export Licence (Cryptographic Development)' (UK Government, 20 January 2017).
[607] Privacy International, 'The Global Surveillance Industry', July 2016, p.31.

The decision over whether to export surveillance software is made by the Secretary of State in the DiT, with input from other government departments. At the time of writing the UK had eight criteria, updated in March 2014, which aimed to capture both international obligations and specific national requirements.[608] The second criterion concerns "the respect for human rights and fundamental freedoms in the country of final destination", and a licence will not be granted if there is a "clear risk that the items might be used for internal repression". 'Might' is then clarified as "evidence of the use of these or similar items" or "reason to believe the items will be diverted from their stated end use" for internal repression. A 2017 court judgement on transfer of weapons to Saudi Arabia elucidates the 'clear risk' criterion, based on an EU User's Guide, as including the recipient's record of respect for international humanitarian law and their "intentions as expressed through formal commitments".[609] It states that incidents violating humanitarian law are not necessarily indicative of the country's attitude, although patterns of violations or lack of punishment for violations "give cause for serious concern".[610]

Despite the extensive incorporation of human rights into the UK's export control regime, the threshold for preventing exports based on human rights concerns is very flexible. First, the human rights criterion is based on risk, which transforms ethical judgements into a probabilistic analysis (doubly so when combined with the phrase 'might'). The introduction to the criteria states that a 'purely theoretical breach' should not prevent exports; as all probabilistic analysis is necessarily theoretical rather than actual, this qualification instead subjectively raises the threshold of prevention. However, the key element of flexibility is in the risk calculation itself.

The court judgement above argues that whether such risk is clear is a question on which there can be reasonable disagreement, and the court gives wide latitude to the secretary of state in making this decision, raising the threshold still further. It also suggests that, to present a clear risk, there must be an established *pattern* of human rights violations, which even then that would only

[608] UK Parliament, 'Written Statement by Secretary of State for Business, Innovation and Skills (Vince Cable) on Consolidated EU and National Arms Export Licensing Criteria' (UK Parliament, 25 March 2014).
[609] Lord Justice Burnett and Mister Justice Haddon-Cave, 'Judgement on Campaign Against the Arms Trade Application, [2017] EWHC 1726 (QB)' (Royal Courts of Justice, 10 July 2017), p.179.
[610] Burnett and Haddon-Cave, p.179.

'cause serious concern' rather than automatically preventing exports. There is not one single UK government view on these thresholds: two separate committees took wildly different stances in the Saudi Arabia case above.[611] Finally, the EU Users' Guide implies that if a recipient state makes formal statements, joins international bodies, and so on, this diminishes the judgement of risk. It is therefore advantageous for recipients to do so, even if their commitment is merely skin-deep.

The dynamics of decisions on cybersecurity exports were well summarised by Jonathan Shaw, former head of cybersecurity at the UK Ministry of Defence, in an interview for the BBC. Shaw stated that:

> It's a trade-off … I would imagine the consideration that plays in people's minds is not so much the economic advantage... but it's that the security of the state we're talking to is closely linked to ours. Or they are tracking people who are a direct threat to Britain and we need their assistance.[612]

Shaw here characterised the risk framework of the export regime as being a trade-off between human rights violations and security concerns. This is not officially the case; the opposite in fact, as export controls specify that the human rights criterion *cannot* be weighed against national security. Nonetheless, the trade-off is there, hidden under a more complex risk framework where the judgement of likelihood, consistency and severity allow it to be made in a private, classified manner by the secretary of state. The risk calculations of this export regime essentially build in flexibility, assimilating both human rights and national security in a way which enables decisions to go either way depending on economic incentives. Exporting states thus keep an image as 'steward states' of human rights, while also facilitating the sale of surveillance equipment.

***

This chapter has demonstrated that surveillance suppliers perform the moral manoeuvre of manipulation: assimilating both organisational and human rights values under a wider risk

[611] John Stone, 'Britain's Arms Control Committee Can't Agree What to Do about Selling Bombs to Saudi Arabia', The Independent, 15 September 2016, https://perma.cc/QBZ8-FXYR.
[612] BBC, 'How BAE Sold Cyber-Surveillance Tools to Arab States'.

framework in a way which retains flexibility, allowing them to both maintain or halt exports in different situations. This moral manoeuvre assimilates multiple value clusters agnostically, without normative commitment to any of them. Norm-based explanations of the empirical data in this chapter do not adequately recognise the extent to which these suppliers are active and strategic participants in shaping as well as responding to international norms like the Wassenaar Arrangement. These actors do not progress through successive levels of socialisation, but instead manipulate the socialisation process itself, especially structures of abuse and misuse, to achieve their economic goals. However, while this chapter has investigated the pressures around international norms for surveillance suppliers clearly engaging with such norms, even if in a calculated manner, it has not addressed the value orientations of the wider cybersecurity industry outside this specific group. This is the subject of the last empirical chapter, focusing on the moral manoeuvre of *elision*.

Chapter 9. Elision

In a presentation at the Arab Region Cybersecurity Summit in October 2016, the presenter explained the ways in which images could be tracked across the internet, and the amount of data that could be obtained by doing so: the location of the photographer, other images they had taken, their friends and people in the same location when the picture was taken, and so on. The presentation used one specific image as its case study: a photo taken by a protester in the Arab Spring of January 2011. The presenter proceeded to list the other demonstrations this individual had attended, other people near him in these demonstrations, and a swathe of details of both the online and offline profile of this individual, down to the type of camera and mobile phone he owned, all based on one image. When I asked other attendees why he had used that specific example, the reaction was an uncomfortable silence, before one shrugged and said, "he has his own reasons".

This presentation was ostensibly an illustration of open source analysis, relevant to cybersecurity organisations because it demonstrated the wealth of data available in the public domain. However, given the audience – including the Egyptian Ministry of Interior and security agencies – it also had an entirely different message. This was a demonstration of a surveillance technique that could be used (and in the example *was* used) to track an individual attending a protest. This presentation highlights the ubiquity of monitoring and data collection as a fundamental practice in cybersecurity. It also illustrates what I term the moral manoeuvre of *elision:* the eliding of differences between different environments in which monitoring takes place. In this case, the image analysis system was presented as a defensive tool, at a conference focused on protecting business and government networks, but the implied use was for the security services to track dissidents.

This chapter traces the moral manoeuvre of elision as performed by actors not directly addressed by the cyber norms considered in previous chapters. Specifically, it focuses on three sets of actors that are not within the scope of the Wassenaar Arrangement: specialised cybersecurity companies (whose activities are deliberately excluded from the amendment); local surveillance suppliers and resellers (who are not based in countries covered by the Arrangement); and local telecoms companies (who engage in surveillance but do not export it). Whereas the three moral

manoeuvres detailed in previous chapters complemented or extended norm-based explanations, highlighting dynamics that are understated or missed in those accounts, elision is performed by actors that are bypassed by such accounts. This thesis therefore not only provides a better explanation of how cybersecurity actors relate to existing cyber norms, but also shows how commercially motivated actors alter values in cybersecurity outside such norms.

This chapter is structured as follows. The first section demonstrates how cybersecurity knowledge in the region is shaped by cybersecurity companies and local resellers, including through the sponsorship of cybersecurity conferences. The second section shows how conference presenters use portable cybersecurity concepts to sell their services to a wider audience, eliding differences between national security and commercial environments. The third section analyses how local telecoms companies use these concepts to conduct censorship and surveillance.

9.1 The cybersecurity industry

The cybersecurity industry underpins the professional community in Egypt and the Gulf states. As reflected in the interviewee characteristics detailed in Chapter 4, nearly all cybersecurity professionals had previous private sector experience or worked in the private sector at the time of interview. In this section I focus on specialist cybersecurity companies and their closest competitors. The argument of this section is that these companies play a key role in the production of cybersecurity knowledge. This premise underpins the moral manoeuvre of elision, as the portable concepts used in elision gain salience due to the knowledge production practices of these companies.

Clear economic incentives attract cybersecurity companies to the Middle East. The market research company Gartner valued the 2014 'Middle East and North Africa' cybersecurity market at just over $1 billion, rising to $1.3 billion in 2016.[613] Other reports, although using higher values than Gartner, put the region at around 7% of the global cybersecurity market in monetary value.[614] Health,

[613] Gartner, 'Gartner Says Middle East & North Africa Information Security Spending to Reach US$1.3 Billion in 2016', 31 October 2016, https://perma.cc/3LWW-GUGP.
[614] Micromarketmonitor, 'Middle East and Africa Cyber Security Market Research Report | MicroMarketMonitor.Com', 2015, https://perma.cc/3EV9-PFDE.

finance, and energy sectors feature heavily in market analyses. The GCC overall, and UAE and Saudi Arabia in particular, are commonly highlighted as regional targets: the UAE due to its positioning as a global business hub, and Saudi Arabia due to its relative population size and large oil reserves even relative to the GCC. Consequently, this section focuses mainly on the UAE and Saudi Arabia. As detailed in Chapter 3, there are significant differences between the economies of the GCC states and Egypt and also many intra-GCC differences. It should be noted that the companies treated in this section are only one part of the wider industry. By 2017 most big IT companies, such as IBM, Microsoft, and HP, as well as consultancies such as EY and Accenture, all had cybersecurity advisory departments and either repackaged or designed their own cybersecurity products.

Interviewees highlighted the importance of international financial flows to cybersecurity, and the discrepancy in perceptions of those flows from different subject positions. On one hand, a stereotypical view of Gulf wealth was taken by several Western cybersecurity exporters, who found it difficult to conceal their surprise and excitement in interviews: "It's astonishing how much they spend – how much they are willing to spend. Gulf countries can afford it" (I-32). Another compared it to a piecemeal approach in Europe: "Here people would buy the whole lot, and you are like 'wow!'" (I-13). This was tempered somewhat by the 2015 collapse in the oil price, with several interviewees recognising that "the big problem is oil price and budgets… those at the top don't want to carve out the money for cyber" (I-25).

On the other hand, GCC nationals disagreed strongly with this view of unending wealth. One put it starkly, saying that "we are a big ATM machine, that's the wrong concept people have… they come for money, not for research" (I-40). Another confirmed this imbalance: "The vendors make lots of money… And here it is all sales teams, they do not do development" (I-12). Some emphasised their careful spending - "we don't have an open cheque" (I-17) - but others disagreed: "The management never tell me no for cybersecurity purchases, even with oil price difficulties" (I-54). These quotations suggest that both companies selling cybersecurity products and their customers are aware of the global economic flows that motivate this encounter. The overarching motivation for these companies, therefore, is an economic goal, as in the previous chapter.

Some interviewees argued that cybersecurity sales can only take place after a process of education, creating a professional community in the region who would understand the necessity and urgency of cybersecurity. As one interviewee explained, "people here are not tech savvy, you need to teach them what to think" (I-50). Another said his purpose was to ensure that customers "would be properly educated in our view of cybersecurity" (I-42). One interviewee, a UK national, claimed that technical prowess was a key aspect of cybersecurity expertise:

> I have seen in the Middle East that expert technical people profile better over there than here; if you've done it, and you've seen the world, that can have a disproportionate impact compared to doing all the bowing and scraping and acting well relative to their morals. If you're a technical expert then they hang off your every word (I-41).

This quotation and the others above suggest that cybersecurity companies in the region deliberately combine both product sales and knowledge production, although it is not within the scope of this thesis to explore the culturally essentialist assumptions and quasi-colonial power dynamics that underlie these quotations.

The symbiosis between professional knowledge and profit is demonstrated especially by Symantec, the cybersecurity company with the longest history in the region. Symantec originally sold antivirus and system recovery software under the Norton brand, as well as firewalls after it acquired Axent in 2000. Symantec made large acquisitions in the main period examined by this thesis, as it bought Verisign in 2010 for $1.3 billion and Blue Coat – a provider of traffic management and filtering mentioned in Chapter 6 – in 2016 for $4.5 billion. In 2015, Symantec also acquired staff from Narus, a traffic management and surveillance company, which was then a subsidiary of Boeing.[615] Other Symantec partners included Deloitte in 2014 and Dark Matter, a UAE-based intelligence supplier, in 2016.[616] Symantec's product line expanded with these acquisitions and partnerships to a comprehensive service, although its core business remained endpoint protection.

[615] Zachary Fryer-Biggs, 'Symantec Buying Technology and Hiring Cyber Experts from Boeing', *Jane's Defence Industry* 32, no. 2 (1 February 2015).
[616] PR Newswire, 'DarkMatter and Symantec to Provide Next-Generation Cyber Security Solutions and Services' (PR Newswire, 27 April 2016).

Symantec's activity in Egypt and the Gulf states pivoted around its offices in Dubai and Riyadh, which opened in 2002.[617] Symantec offered managed security services in 2004 with local partners in Saudi Arabia,[618] including security education in Arabic.[619] In the UAE, Symantec struck a partnership with government-owned telecoms provider Etisalat in 2005.[620] Around the same time, Symantec also agreed a partnership with MaxSecure, a UAE startup, described as follows:

> The partnership was first initiated by Dr. Omar Bin Sulaiman – CEO of Dubai Internet City at the time and… a board member of Mohammed Bin Rashid Establishment – who identified a synergy between MaxSecure and Scanit. Dr Bin Sulaiman, who was actively looking for ways to support and build up technology business startups being incubated at the Mohammed Bin Rashid Establishment for Young Business Leaders, highlighted the strategic importance of technology knowledge transfer from Scanit and Symantec to MaxSecure.[621]

Symantec thus followed the advice of a well-connected member of the UAE elite to transfer not just technology but 'technology knowledge'. Symantec's training activities in the UAE then went further, as the company was contracted to create aeCERT itself in 2007. Business media reported that "the contract awarded to Symantec will include actual recruitment and training, building the expertise, and the hands-on system";[622] in other words, what one of the interviewees above described as "building an educated customer" (I-42). Given these links, the creation of the cybersecurity expert community in the UAE and Saudi Arabia has been significantly shaped by Symantec's own perspective on what constitutes cybersecurity and what technical tools are required to improve it.

Other cybersecurity companies matched Symantec's focus on training and education. Kaspersky, a Russian antivirus company, has a longstanding and substantial presence in Egypt and

[617] Middle East Company News, 'Symantec Expands Middle East Operations.' (AME Info, 13 January 2002).
[618] Al-Bawaba News, 'Symantec Announces Appointment of IMT as First Managed Security Services Partner in Saudi Arabia' (Al-Bawaba, 16 May 2004).
[619] Middle East Company News, 'Symantec Announces Fully Arabized Education Services Tool for Improved Corporate Security' (AME Info, 5 October 2004).
[620] Middle East Company News, 'ECompany Signs Alliance with Symantec to Improve Internet Security in the UAE' (AME Info, 11 January 2005).
[621] Middle East Company News, 'Mohammed Bin Rashid Establishment for Young Business Leaders Company in Partnership with Symantec and Scanit' (AME Info, 23 May 2005).
[622] Xinhua News Agency, 'UAE to Establish Computer Emergency Response Team' (Xinhua, 30 August 2007).

the GCC states.[623] In 2008 Kaspersky launched an Arabic edition of its antivirus software.[624] In 2009, it began a regional expansion strategy, albeit with only 10 people in its office.[625] As part of this strategy, Kaspersky launched a training centre in cybersecurity in Dubai Knowledge Village.[626] Kaspersky's attempts to install alternative centres of knowledge production highlights the commercial value these companies attach to such practices.

Larger IT companies, including Cisco, Intel, and Dell, also focused on knowledge production. Cisco's presence in the region goes back a relatively long way in cybersecurity. It opened a regional office in Dubai in 1995,[627] and in 1998 held seminars for Middle East clients on how to connect to the internet safely.[628] In terms of education, Cisco was also involved relatively early on in this region: it partnered with Etisalat Academy from 2002 and set up the first Middle East IT security conference at this time.[629]

Intel followed a similar trajectory. In 2010, Intel sponsored the Kustar Discovery Centre, focusing on new technologies including cybersecurity, at Khalifa University in Abu Dhabi.[630] Intel's main move into cybersecurity was through the acquisition of antivirus firm McAfee in 2011 for $7.8 billion. McAfee then set up a Cyber Defense Center in Dubai in 2013, which offered incident response, forensics and security education.[631] Ambitiously, it claimed that "the centre, with 10 staff, has been collecting intelligence for the past nine months and will attempt to pro-actively warn institutions when they are perceived to be under threat."[632] The combination of cybersecurity

[623] Middle East Company News, 'Kaspersky Lab Expands Its Middle East Outreach with Fusion Distribution' (AME Info, 23 January 2007).
[624] Middle East Company News, 'Kaspersky Lab Launches Arabic Edition of New Anti-Virus and Internet Security Products in Mideast' (AME Info, 17 November 2008).
[625] Middle East Company News, 'Kaspersky Lab Middle East in Regional Expansion' (AME Info, 9 July 2009).
[626] Middle East Company News, 'Kaspersky Lab Launches First Middle East Authorized Training Centre' (AME Info, 1 June 2009).
[627] Kinda Jayoush, 'Cisco Sees Potential for Middle East Growth' (Reuters, 27 July 2000).
[628] The Star, 'Internet Security & Web Scaling from CISCO' (WorldSources Online, Inc., 10 December 1998).
[629] Middle East Company News, 'Cisco Advances Its Integrated Security Strategy' (AME Info, 25 February 2003).
[630] Middle East Company News, 'HH Sheikh Hamed Bin Zayed Al Nahyan Launches Kustar Discovery Centre in Abu Dhabi' (AME Info, 4 July 2010).
[631] Islamic Finance News, 'McAfee Selects Dubai to Launch Its First Cyber Defense Center' (Contify, 3 September 2013).
[632] Courtney Trenwith, 'McAfee Opens Its First Cyber Defence Centre in Dubai', ITP.net, 3 September 2013, https://perma.cc/JER3-BWL4.

consultancy services, including threat intelligence, with security education was a key part of Intel and McAfee's strategy in the region.

Finally, Dell – originally an IT hardware manufacturer – moved into cybersecurity in 2011 with the acquisition of SecureWorks for $612 million. Dell then also bought SonicWall, a firewall company, in 2012 (which it sold in 2016). Dell also works in law enforcement: it provided Sharjah police in the UAE with a new data analysis system for their surveillance cameras,[633] and in 2011 worked with Microsoft and a specialist surveillance company to provide intelligence analysis for governments at an Abu Dhabi defence trade fair.[634] In 2015, its main Middle East markets were in Egypt, UAE and Saudi Arabia.[635] Dell then completed a massive acquisition of EMC2, which owns RSA, a cybersecurity events and software company, in 2015 for $67 billion. The first major RSA cybersecurity event in Abu Dhabi then took place in 2016 (although smaller-scale events had taken place earlier). RSA is widely seen as the professional standard of cybersecurity conferences globally and its arrival in the UAE set a baseline for cybersecurity knowledge in the region.

One way of highlighting the role of cybersecurity companies in the creation of expert knowledge is through an analysis of sponsorship of the 165 cybersecurity conferences detailed in Chapter 4. The top twelve companies are detailed in Table 9.

Table 9: Sponsorship of cybersecurity conferences

Company ("+" denotes subsidiaries included)	No. of conferences
Raytheon+	15
Dell+	15
Qualys	14
HP	14
BAE	13
Help AG	11
Cisco	11
Global Security Network	10
F5 Networks	10
Symantec+	9
Fortinet	9
Kaspersky	9

[633] Arabian Business, 'Sharjah Police to Update Surveillance Infrastructure' (ITP Business Publishing, 11 September 2014).
[634] Trade Arabia, 'Olton to Launch Improved Intelligence System' (Al Hilal Publishing, 24 February 2011).
[635] New Vision, 'Dell to Partner up with Middle East Firms to Build Cloud Services' (New Vision, 26 October 2015).

This table suggests that although no one company sponsors anywhere near a majority of cybersecurity conferences in the region, companies that have a significant economic stake in regional cybersecurity sponsor the most conferences. This includes the defence companies Raytheon and BAE, considered in the previous chapter, and nearly all the cybersecurity companies above (Intel/McAfee was in 19th place, sponsoring 8 conferences). Conference sponsorship usually means a speaking slot and thus a chance to promote the company's products to the professional community.

Some of the other main conference sponsors are resellers of cybersecurity products. Resellers are a crucial aspect of the market in the region and their cybersecurity activity is often part of a wider IT distribution chain. For example, Help AG, originally founded in Germany in 1995, has been present in the Middle East since 2004 and has headquarters in Dubai.[636] It resells Symantec products as well as products by cybersecurity companies like Palo Alto, Tenable, F-5 Networks, and Juniper. ComGuard is another major distributor in the region, and has worked with HP and Kaspersky, as well as Juniper and Qualys. It was founded in 2002 and is also headquartered in Dubai.[637] Finally, Starlink is a distributor for Dell, Cisco, and many others, and was founded in 2002 in Dubai.[638] Starlink has worked with many business and government clients in Saudi Arabia, including the Ministry of Foreign Affairs.[639]

These resellers are an important link because of their familiarity with the local environment. Interviews suggested that this familiarity included activity which could be an offence under anti-corruption legislation in the US or Europe. As one British exporter said:

> Having a 2nd tier [i.e. a reseller] abstracts you from these bribery type problems. All Western companies do this, and it also gives you the technical reach and a BD [business development] manager, who is important. He will have lots of vendor products, and sells them all on commission, so you need him to be on side… You need a partner with the best relationship with the customer. Because of this, there are lots of grey areas with the UK bribery act and the FCPA [Foreign Corrupt Practices Act] (I-47).

[636] Help AG, 'About Us - the Company' (Help AG, 2016), https://perma.cc/K3MY-YKPL.
[637] Comguard, 'About Comguard' (Comguard, 2014), https://perma.cc/T55Q-K3GY.
[638] Starlink, 'Starlink Celebrates 10 Years as the Region's Trusted Security Advisor', StarLink, October 2015, https://perma.cc/H5JQ-K56W.
[639] Wikileaks, 'The Saudi Cables Doc#129897 FW: MOFA - Fireeye', Wikileaks Forum, 12 February 2015, https://perma.cc/WKF3-KGGV.

This quotation suggests that the specific capabilities of the cybersecurity technologies are less important than the cultivation of personal relationships through both legal and illegal means. This has echoes of investigations of corruption in historic arms deals in the region by several defence companies now involved in cybersecurity.[640] A different interviewee noticed a similar process in Qatar:

> Sales are not about the strength of the product: here, that doesn't matter at all. I have seen it happen myself, it's all about connections and knowing the right person. You have a network, if they know you and trust you then they do the deal. It is all about personal relationships. Raytheon sell here in Qatar, and their reseller is a company with a Qatari head… and he makes a lot of money, as the contracts are billions. It's all about the person you have in the middle (I-12).

If this is accurate, then it paints a slightly different picture of the relationship between the creation of professional knowledge and economic incentives underlying the establishment of cybersecurity companies in this region than the references to 'building a customer' quoted earlier. Rather than teaching local experts the knowledge necessary to make an informed decision about the best product for them (whatever the power dynamics within this relationship), security education, training centres, and conference presentations offer cybersecurity companies the chance to *perform* as a cybersecurity expert in front of potential clients. This performance, irrespective of its content, maintains the relationships necessary for sales, rather than passing knowledge to the customer. As one interviewee put it: "It is a bit contradictory – you have to show them issues, but not too deeply" (I-31).

Some sources suggest that market success can be more a question of the right political connections. An Intelligence Online report detailed relationships between Muhammad Al-Nayef, the former Saudi Minister of Interior (see Chapter 7, Section 3) and cybersecurity companies as follows:

> In the space of a few years, Nayef has established a close relationship with the local cyber-security industry in Saudi Arabia. Al-Elm Information Security, one of the sector's market leading companies in Saudi Arabia, was founded by Khalid al-Tawii. The latter was Nayef's personal advisor on cyber-security for a long time. He most notably headed the secret Saudi-US technical security programme, including a critical infrastructure cyber security programme, that was launched in 2009 and he was also involved in the creation of the ministry's dedicated Diplomatic Security Service (DSS).[641]

[640] Nicholas Gilby, *Deception in High Places: A History of Bribery in Britain's Arms Trade* (London: Pluto Press, 2014).
[641] Intelligence Online, 'Mohammed Bin Nayef Pursues Cyber Ambitions', 17 February 2016, https://perma.cc/NUJ2-CV68.

I confirmed with interviewees that Al-Elm is contracted to perform confidential national security work for the Ministry of Interior, and partners with external vendors to do so (I-49). However, the Intelligence Online report goes further:

> Al-Elm has several computer security contracts with Nesma, a company owned by Saleh Ali al-Turki. Nesma is also active in cyber business with the defence ministry via its sister companies Pannesma and Saudi Prerogative Co. Qwaed Technologies is another cyber company that is close to Nayef. Qwaed, which works most notably for the conglomerate SABIC, is sponsored by Mohammed bin Saud bin Nayef, the son of Saud Bin Nayef, the interior minister's elder brother.[642]

I was unable to verify these connections independently, and this is a single source to be treated with caution. However, if this report is accurate, then familiarity with the local business environment would not be the only reason to engage a particular reseller or local partner. Their ability to secure sensitive government contracts as well as private sector work may also be a factor.

Overall, this analysis of the cybersecurity industry has shown how cybersecurity companies look to maximise their sales in several ways: through creating knowledge, engaging resellers, and building influential relationships. Their overall motivation is to sell their products and services, but they also play a key role in defining cybersecurity expertise in the region itself.

9.2 Portable concepts

This section investigates the moral manoeuvre of elision, demonstrating how values and technical claims are altered at conferences in the region sponsored by the cybersecurity industry. In the preceding chapters I distinguished an explanation in terms of moral manoeuvres from one in terms of cyber norms, based on the amended Wassenaar Arrangement controlling dual-use technologies. However, the cybersecurity companies analysed in this chapter are neither advocates for the Wassenaar amendment nor do they fall within its scope. There is therefore no clear norm-based explanation for the data presented here.

[642] Intelligence Online.

This section returns to the question of dual-use present throughout this thesis. To recap, in Chapter 6 I focused on the concept of dual-use from the perspective of the NGOs who aligned human rights values with the organisational conception of cybersecurity. In Chapter 8, the concept of dual-use appeared again in the way surveillance suppliers manipulated the values underlying the legitimate use and the potential misuse of their technologies. I build on these discussions to emphasise that although the potential for multiple uses is rooted in the affordances of the technologies themselves, it is also socially and organisationally entrenched.

A key aspect of elision is the production of what I call 'portable' concepts, able to travel between both national security and commercial environments. In national security environments, the networks to be protected are those of the state as a whole, whereas in commercial environments it is the networks of a specific company or organisation. Portable concepts *elide* differences in the relevant values between these two environments, enabling cybersecurity companies to reach a wider potential market.

The distinction between national security and commercial cybersecurity environments is akin to another much-discussed distinction in cybersecurity, between 'offensive' and 'defensive' actions, which deserves brief clarification. The standard distinction between offensive and defensive actions in cybersecurity is between penetrating the networks of others (offence) and protecting your own networks (defence). Based on this distinction, cybersecurity is widely believed to be 'offence-dominant': it is easier to attack networks than defend them. This is in fact highly dependent on the capabilities of the attacker and defender: there is no general rule.[643]

The distinction between offence and defence features prominently in what Buchanan calls the 'cybersecurity dilemma' (not the same as Dunn Cavelty's concept with the same name treated in Chapter 2). A cybersecurity dilemma is where the penetration of one state's networks by another state for surveillance is mistaken for preparation for an 'attack', creating an escalatory dynamic between those states. Buchanan uses traditional IR concepts of offence and defence rather than the specifically cybersecurity sense above: offence causes harm, rather than simply being the penetration

[643] Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41, no. 3 (1 January 2017): 72–109.

of others' networks whatever the result. Consequently, both horns of his cybersecurity dilemma are offensive in the narrow cybersecurity sense.[644] Other scholars have argued that the offence/defence distinction should be replaced by a focus on deception.[645]

This distinction is relevant because both national security and commercial environments have offensive and defensive elements. In national security environments, offence is acting outside the state and defence is protecting networks inside the state, while in commercial environments offence and defence imply respectively acting outside the company or inside the company.[646] Given the lack of clarity over the difference between offence and defence in cybersecurity, I use the simpler distinction between national security and commercial environments.[647] In this section I treat two portable concepts in detail, network visibility and insider threats, and then consider their combination by UAE company Dark Matter.

9.2.1 Network visibility

Network visibility is a common concept in the cybersecurity industry, meaning simply the ability to monitor traffic anywhere on a network, whether on central servers or between 'endpoints', the devices used to connect to the network. The term gained prominence in relation to intrusion detection and prevention systems sold by the specialised cybersecurity companies detailed in the previous section. Network visibility is a key advantage of these systems, as they automatically process large volumes of traffic, identifying (and, if requested, modifying) anomalous behaviour. Network visibility, in commercial environments, applies to the specific networks of the client company or organisation.

---

[644] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst, 2017).
[645] Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* 24, no. 2 (3 April 2015): 316–48.
[646] Lucas Kello, 'Private-Sector Cyberweapons: Strategic and Other Consequences', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 15 June 2016), https://papers.ssrn.com/abstract=2836196.
[647] Both private and public-sector actors can be in either: private sector actors can work at a national level, and state actors can work to secure company networks.

At the annual Arab Region Cybersecurity Summit in Muscat in 2017, a keynote address by an FBI special agent also used the concept of 'network visibility'. His presentation extended this concept to the state itself, saying that "at the national level we need to have full visibility into our networks, to prevent data from being taken or sent". This extended concept of network visibility would require the sort of surveillance systems described in the previous chapter. (Incidentally, in an implicit reference to Snowden, another presenter immediately joked that "I find it funny that we are listening to the FBI on how to protect our data". This remark was studiously ignored by the FBI agent.) The FBI agent thus transferred this technical concept from a commercial environment to a national security one.

Later the same day, a reseller of cybersecurity and surveillance technologies presented on the same stage. In his presentation, he provided an overview of his business model, as follows:

> Ministries of Justice in the region have problems when someone insulted someone else on FB or Twitter, then he deleted it. We keep it all to help you reach the right conclusion. We can identify users' interests and relations. I'm a terrorist in a mall, communicating with others, we can see this and you can build connections in real time (ARCS2017).

The swift movement from online insult to a terrorist attack highlights the appropriation of cybersecurity and cybercrime considered in Chapter 7. However, more relevant to this chapter is that he described his technologies as providing 'network visibility'. I was intrigued by his use of this term and asked him after his presentation why he chose that description. He responded: "you need full network visibility. The FBI man said that at the end of his presentation, and he is right, so I put it into mine." This is a crucial quotation, demonstrating the portability of the concept *in action*. Network visibility first moves from a commercial environment to a US national security environment, and from there to the expanded version of national security present in Egypt and the Gulf states. This movement occurred *in* cybersecurity conferences, as cybersecurity experts listened to and borrowed technical concepts from each other.

This presenter's company, as a local reseller, is not subject to the Wassenaar Arrangement controls, as this company is not based in a state within the Arrangement. Nonetheless, when I spoke to this presenter, he emphasised his ethical stance:

> We do everything by the book. It is about ethics, and what you are willing to do. I have lost contracts with private companies because I refused to provide something that I would only give to governments. It is up to the person using the technologies how they are used. We sell it, we train people, and then they use it. They have to be ethical in how they use it (ARCS2017).

As well as eliding differences between commercial and national security environments through the concept of network visibility, this reseller here also echoed the manipulation of human rights values performed by Hacking Team and the other surveillance companies examined in the previous chapter. This included a clear profession of 'ethical' behaviour and distance created by his role as a mere technology provider. This conversation suggests that actors outside the scope of the Wassenaar Arrangement engage in multiple moral manoeuvres simultaneously; however, this combination is not within the scope of this thesis, and I return to it as an avenue for future research in the conclusion.

9.2.2 Insider threats

Another portable concept is that of the 'insider threat'. The concept of an insider threat has a long history in intelligence and espionage and is often seen as synonymous with 'spy': an individual who operates within an adversary state to obtain information to help another state.[648] The concept of insider threat is very salient in Middle East cybersecurity. A 2016 cybersecurity survey by consultancy company PwC on the Middle East highlighted insider threats, saying that "while companies in the region are acutely aware of the threat posed by insiders, only 38% perform proper background checks on their personnel, against 51% globally."[649] This view also appears regularly in cybersecurity conferences in Egypt and the Gulf states. For example, a spokesman for a US defence company, Booz Allen Hamilton, said at a conference in 2012 that insider threats were third on his list of top cyber threats.[650] In a press interview for another conference in 2012, a UK-based consultant

[648] Federal Bureau of Investigation (FBI), 'The Insider Threat', 10 February 2014, https://perma.cc/MF4D-FG68.
[649] PwC, 'A False Sense of Security? Cybersecurity in the Middle East' (PwC, March 2016), p.10.
[650] Madhuparna Bhattacharjee, 'Cross-Border Collaborations Can Tackle Cyber Security', Muscat Daily News, 2 April 2012, https://perma.cc/6VLC-XXQE.

summarised the top cybersecurity threats as "other nation states, criminals, terrorists, hackers and even disgruntled employees".[651]

Cybersecurity insider threats have several conflicting definitions. First, insider threats are usually defined to include organisations in both the public and private sector. As Nurse et al. explain, "an insider can be thought of as an individual who is an employee (past or present), contractor or other trusted third party, who has privileged access to the networks, systems or data of an organisation."[652] However, cybersecurity professionals have widened the concept of insider threat further.[653] Nearly all cybersecurity incidents involve apparently legitimate communications: as the cybersecurity scholar Martin Libicki memorably put it: 'there is no such thing as a forced entry in cyberspace".[654] Consequently, for many cybersecurity professionals, the concept of an insider is broader than its pre-cyber versions, denoting not only a malicious or negligent individual but also a deceived employee or 'accidental threat'. In the words of the Carnegie Mellon University CERT, an accidental insider threat is "an insider who, without malicious intent and through action or inaction, causes harm or increases the probability of future harm to the… organisation's assets or resources."[655]

These different senses of insider threat are often conflated. For example, another PwC report in 2013 slid easily from a narrow 'malicious' definition to one that encompasses all of the above elements, saying that:

> Insiders can act alone, or under the influence or direction of one of the other threat actors, and they are often motivated by revenge or financial factors. Indeed, oil and gas respondents to PwC's annual security survey reported that current employees comprise the most cited likely source of security incidents (40%).[656]

---

[651] Adam Lane, 'Countdown to Abu Dhabi Cyber Security Forum', utilities-me.com, 10 May 2012, https://perma.cc/2U96-L6B5.
[652] J. R. C. Nurse et al., 'Understanding Insider Threat: A Framework for Characterising Attacks', in *2014 IEEE Security and Privacy Workshops*, 2014, p.214.
[653] It is often conflated with a specific tactic called 'social engineering'.
[654] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2010), p.35.
[655] Nurse et al., 'Understanding Insider Threat', p.214.
[656] PwC, 'Embedding Cybersecurity into the Energy Ecosystem: An Integrated Approach to Assessing Cyber Threats and Protecting Your Assets' (PwC, February 2013), p.4.

This conflicted understanding of insiders permeates the commercial cybersecurity environment. A McAfee report in 2015 stated that 43% of data breaches were due to internal factors, half negligent and half malicious.[657] A survey in 2017 raised this percentage to 74% by including current and previous employees, customers and suppliers.[658] Another industry survey, sponsored by Siemens, concluded that negligent insiders were more of a threat than malicious ones: "sixty-one percent of respondents say the top cybersecurity threat is the negligent or careless insider, underscoring the need for advanced monitoring solutions to identify atypical behaviour among personnel."[659] Some cybersecurity companies even define insider threats to include remote hackers who merely *appear* to be employees. For example, a 2016 Mandiant report advised that "investigators must hunt for threat actors posing as 'an insider'; using legitimate credentials to blend in with normal user activity".[660] The key point here is that multiple meanings of insider threats only partly stem from the underlying technologies. This multivalence is also due to conceptual work undertaken by cybersecurity experts *producing* professional knowledge.

The concept of 'insider threat' at the cybersecurity conferences I attended highlights the portability of the concept in the cybersecurity profession more generally. For example, the keynote speaker at RSA Abu Dhabi in 2016 claimed that "the insider threat could be malware or someone who's stolen your credentials" (RSAAD2016). More specifically, at a conference in Dubai shortly after RSA Abu Dhabi, there was a panel discussion focusing on the insider threat where the presenters wrestled with these distinctions. The relevant part proceeded as follows:

[657] McAfee Labs, 'Grand Theft Data: Data Exfiltration Study - Actors, Tactics and Detection' (Intel, September 2015), p.4.
[658] Hannah Simms, 'Insider Threats Make up 74% of Business Cyber Security Incidents', IT PRO, 22 September 2017, https://perma.cc/KYR5-GMHV.
[659] Ponemon Institute LLC, 'The State of Cybersecurity in the Oil and Gas Industry: Global' (Siemens, March 2017), p.3.
[660] Bill Hau et al., 'M-Trends 2016 EMEA Edition' (Mandiant Consulting, June 2016), p.6.

> *Panellist 1:* Both the person conducting the attack and the targeted person are human, so the term 'weakest link' is confusing. Most attacks get in through weak implementation, through misconfiguration or new applications.
> *Panellist 2:* Humans may target you intentionally, and that's where the insider threat comes in. We do a much more thorough background check and more ongoing monitoring. We have been able to prevent IP [intellectual property] loss through doing this.
> *Panellist 3:* Most attacks come through the human factor.
> *Panellist 4:* We have to protect CEOs - they are the most important people, as they have to know everything. More than 80% of cyber attacks are internal, in that they collude with attackers.
> *Panellist 2:* Yes, hacktivism, people have strong opinions and they want to stick to it. Or they have grudges, or they are stealing IP. But we can't ignore the unintentional human hacking, like checking on a link or plugging into a USB.
> *Panellist 4:* Nobody does it deliberately, but it can happen anyway.

These panellists switched between different definitions of the insider threat within seconds of each other. Panellist 2 put forward an intentional definition of insider in their first comment, and then expanded it to include 'unintentional human hacking' in their second comment (supported by Panellist 1 and 3). Panellist 4 cited statistics similar to those above blaming cyberattacks on 'internal' factors and collusion, implying intent, and yet then maintained that such actions were unintentional.

This conceptual elasticity means that insider threats can be used to refer to almost any cybersecurity incident. As noted in the discussion of Shamoon in Chapter 5, that incident was understood immediately as an insider threat due to the use of employee credentials, displaying precisely the confusion highlighted here. In that case, the consequences were significant, enabling media sources to speculate that an Iranian agent worked within Saudi Aramco, and putting pressure on investigators to deny their employees' culpability.

Crucially, this elasticity also makes the concept of insider threat highly portable between national security and commercial environments. Companies use the concept of insider threat to motivate the marketing of surveillance technologies originally developed in a national security environment for commercial customers. Defence company BAE Systems offer a tailored insider threat platform and describe its functionality in the following way:

> There are many challenges when it comes to detecting insider threats, particularly as it deals with human behaviours and varying motivations. To manage them effectively, companies need to go beyond technical metrics and security infrastructure. This includes leveraging big data analytics and threat intelligence solutions, thereby complementing their existing defences with proactive behavioural analysis to improve security and reduce risks.[661]

These 'big data analytics' and 'proactive behavioural analysis' are exactly what is offered by their national-level surveillance technologies sold to the Gulf states, detailed in the previous chapter. Similarly, Symantec's acquisition of Blue Coat (which they marketed as "defining the future of cybersecurity", but perhaps not in the way described here) focused on insider threats as a key reason for the acquisition: "we will… usher in a new era of innovation designed to help protect large customers and individual consumers against insider threats and sophisticated cybercriminals."[662] Blue Coat is one of the main suppliers of filtering and censorship equipment identified by human rights NGOs, as detailed in Chapter 6.

Rather than transferring commercially developed ideas of network visibility to the national level, in this case the transfer goes in the other direction. The portability of the concept of insider threat, as developed both in the global cybersecurity profession and specifically in cybersecurity conferences in Egypt and the Gulf states, thus entrenches the dual-use potential of surveillance systems by creating a rationale for their application in commercial as well as national security environments. The value differences between these environments are elided not only by the affordances of the technologies themselves, but by also the portable technical concepts used by cybersecurity professionals.

9.2.3 Dark Matter

One UAE company named Dark Matter, founded in 2014, has combined both portable concepts above to market surveillance technologies in both commercial and national security

[661] BAE Systems, 'Managing Insider Threats', BAE Systems | Cyber Security & Intelligence, 21 July 2016, https://perma.cc/TS94-7LYL.
[662] Symantec, 'Symantec to Acquire Blue Coat and Define the Future of Cybersecurity', Symantec Press Room, 2016, https://perma.cc/38YH-NS3H.

environments. Dark Matter is outside the scope of the Wassenaar Arrangement because its surveillance technologies are produced within the UAE, rather than sold to the UAE from a state under the Arrangement framework. An interviewee in NESA, the UAE national cybersecurity agency, attributed the existence of UAE-based companies like Dark Matter to the amendment to the Wassenaar Arrangement, claiming that "most vendors are not doing offensive, as there are a lot of export controls on these companies. The UAE strategy is to have its own companies" (I-26). Norm-based accounts of the Wassenaar Arrangement would highlight state actions in either promoting or resisting the Wassenaar amendment and company actions insofar as they are controlled by this amendment. Companies such as Dark Matter do not feature in this account, and so by showing how they elide differences between national security and commercial environments I extend the theoretical framework of moral manoeuvres beyond norm-based alternatives.

Several cybersecurity professionals mentioned a close connection between Dark Matter and the UAE security services. As one conference presenter put it in conversation, ""Dark Matter are government really, they are just doing what lots of other governments do, like the NSA and finding information on people" (CSC2016). Their founder and former CEO, Faisal Al-Bannai (whose father was a senior figure in the Dubai police), has also commented on Dark Matter's relationships with UAE security services. Al-Bannai has claimed in media interviews that "Ignoring that use [i.e. surveillance], in my view, would be silly… I think tackling that issue and saying, 'what is the right balance,' is the right question."[663] In the same interview he also stated that Dark Matter's motivation for government contracts was economic, saying that "it is a pure commercial transaction with them". Dark Matter therefore clearly operate in both national security and commercial environments, and their public statements suggest their main motivation for doing so is to increase sales.

In 2016, an Italian self-described hacker was approached by an individual who claimed to be working for Dark Matter. This individual asked the hacker to develop a system "capable of intercepting, modifying, and diverting (as well as occasionally obscuring) traffic on IP, 2G, 3G, and

[663] John Gambrell, "UAE Cyber Firm DarkMatter Slowly Steps out of the Shadows," *Times of Israel*, February 1, 2018, https://perma.cc/CU5Y-6T8L.

4G networks".[664] These capabilities are most likely relevant for a national level surveillance system. The recruiter also had links to Verint, who, as detailed in Chapter 8, reportedly provided interceptions equipment to NESA. The hacker refused the offer and justified his decision on human rights grounds, citing the UAE's repressive policies regarding social media and claiming that "freedom of speech is indisputable… it is a basic right that should be granted to anyone".[665]

Crucially, Dark Matter advertised this surveillance system to the hacker as "their most advanced branch of cybersecurity, to the exclusive benefit of national security".[666] This suggests they include national surveillance within their conception of cybersecurity, contributing to the multiple definitions of cybersecurity itself in this region. This description puts advertising slogans describing their 'holistic approach to cybersecurity' in a new light.[667] Holistic cybersecurity, for Dark Matter, makes no distinction between national security and commercial environments.

The recruitment discussion above was founded on the dual-use possibilities of network monitoring systems. The hacker was approached because he wrote an open source network monitoring tool widely used by cybersecurity professionals (named Bettercap), which includes both interception and infection capabilities. This tool is part of the grey area of cybersecurity technologies with surveillance uses, although it would not be controlled by the Wassenaar Arrangement due to its wide availability and lack of specialised mapping and analysis software.

Although the technological possibilities for dual-use form the basis for Dark Matter's operations across national security and commercial environments, Dark Matter also elide the differences between these environments using several portable concepts. Dark Matter was a prominent sponsor of RSA Abu Dhabi in 2016, and in their presentation a Dark Matter employee introduced the concept of 'continuous monitoring':

---

[664] Jason Murdock, 'UAE Recruiting "elite Task Force" of Cyber Experts to Build Mass Public Spying System', International Business Times UK, 4 August 2016, https://perma.cc/E5SC-GK3B.
[665] Moxie Marlinspike, "A Saudi Arabia Telecom's Surveillance Pitch," May 13, 2013, https://perma.cc/GT39-6JL5.
[666] Simone Margaritelli, 'How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People', 27 July 2016, https://perma.cc/EDD3-Y9RZ.
[667] Sarah Rizvi, 'DarkMatter to focus on digital security at GITEX', Channel Post MEA, 25 September 2017, https://perma.cc/GMW9-6RCP.

> Continuous monitoring… what does that mean? So, well, it means what it says really, being able on a continuous basis to monitor your environment, and what you're monitoring is your assets, or hardware and software, your users and your configurations (RSAAD2016).

Users or employees are included here as objects of surveillance, just like programmes or machines. The presenter went on to emphasise network visibility and insider threat, stressing that the concept of continuous monitoring applies as much to unintentional actions as it does to deliberate threats:

> We want to focus on the ability to potentially look at behaviour within the user base so you can identify when there's unauthorised user activity going on – you can call it insider threat, you can call it user behaviour analytics with regards to unintentional activities going on or intentional activities – but being able to look at those different things (RSAAD2016).

In this presentation, a technology developed for national surveillance, by a company founded to avoid export controls on surveillance technologies, was described as a cybersecurity solution for private companies in commercial environments. This is precisely the moral manoeuvre of elision: using portable technical concepts to elide differences between these two environments.

In sum, this section has demonstrated that the cybersecurity industry outside the scope of the cyber norms examined earlier in this thesis also alter values and technical concepts. More specifically, they perform the moral manoeuvre of elision, masking value differences between national security and commercial environments using portable technical concepts to sell cybersecurity technologies in both settings. This moral manoeuvre would not be captured by norm-based approaches, as it is performed by actors who are not directly subject to the norms examined so far in this thesis. Some of these actors, such as the reseller I spoke to, engage with values in similar ways to those within the scope of those norms, whereas others, like Dark Matter, appear to be part of a deliberate strategy to evade such norms. Although elision relies on both the capabilities of the underlying technologies and an organisational foothold in both arenas, it centrally involves the concepts deployed by cybersecurity professionals at cybersecurity conferences.

9.3 Telecoms companies

While the first two sections of this chapter have demonstrated how cybersecurity knowledge is entangled with commercial incentives for specialised cybersecurity companies, and that these companies elide differences between national security and commercial environments using portable technical concepts, there is another actor involved in this moral manoeuvre: telecoms companies. This section details the place of telecoms companies in cybersecurity in Egypt and the Gulf states, and their role in the elision described above.

The role of telecoms companies in elision can only be understood in the context of the liberalisation of the telecommunications sector, which began in the late 1990s. In Saudi Arabia, the national telecommunications agency was privatised to become Saudi Telecom Company in 1998, while Oman did the same with Omantel in 1996. This brought them in line with national companies created earlier in the smaller Gulf states (Etisalat in the UAE in 1976, Batelco in Bahrain in 1981, and Qtel in Qatar in 1987). Each government also created a Telecommunications Regulation Agency to manage this competition. In Egypt, ARENTO became Telecom Egypt in 1998, following a confluence of pressures from US and EU development agencies.

The telecoms sector was further privatised in the early 2000s, with a single national entity split into two or three; however, most still have a substantial government share. Nascent Egyptian mobile networks were also opened to multinationals, creating two networks led by multinational providers Vodafone and Orange. In the Gulf states the mobile networks remained in the hands of the national companies, albeit with smaller stakes taken by multinationals. The main form of competition in the GCC is insular, as the national carriers of each state enter one another's markets, although some, such as UAE's Etisalat, range more widely across the region. National telecoms companies also became the major internet service providers (ISPs) across Egypt and the Gulf states. As part of this move, national telecoms companies funded many transnational undersea internet cables, with a new one every year between 2010 and 2017.[668] On their global route from South Asia to Europe, key

[668] TeleGeography, 'Submarine Cable Map', http://www.submarinecablemap.com/, accessed 16 January 2017, http://www.submarinecablemap.com/.

cables nearly all stop at Egypt, the GCC states, or both. The historic imperial shipping route, with this region as a choke point, is thus recreated for modern internet cables.

Of these companies, the two national telecoms companies in the UAE – Etisalat and Du - have the largest presence across the region and more widely throughout North Africa. Both these companies have the sovereign wealth fund of the UAE, the Emirates Investment Authority, as a majority shareholder. An interviewee in the UAE government provided an indication of their attitude towards their two national telecoms companies. Regarding their entry into the cybersecurity market, he summarised the government's attitude as "we don't want Etisalat and Du to lose, as they are UAE companies… we have to create a market" (I-54). This interviewee suggests that telecoms companies benefit from both government encouragement and preference as well as their unique access to data. This is not unique to the UAE or to cybersecurity; national companies receive preferential treatment in many countries and sectors. However, it is a reminder that the economic situation in which these telecoms companies operate is far from a classical one.

National telecoms companies, especially in the UAE, have exploited their access to data to provide cybersecurity services. One interviewee enthusiastically embraced cybersecurity in the jargon of business consultants:

> Telcos are in a unique position, let's use our connectivity and start security. We can see everything, so let's look at security and extract intelligence… There are lots of horizontals, and new commercial models, but our focus is on the value-add. We are building products, selling products, and doing MSSP [Managed Security Service Provider], we act as a one stop shop for the customer. We're running SOCs as well… We are a telco which is critical infrastructure and an MSSP, so if something happens at a country level we have unique visibility. We can talk to security authorities and customers. (I-38).

This quotation highlights this interviewee's aim to exploit the unique position of national telecoms companies in both the market and the state itself for commercial gain by selling cybersecurity products. The marketing power provided by critical infrastructure was noted by another interviewee, in a different UAE telecoms company, who said that "We are supporting the govt as critical infrastructure… We understand that we can monetise our infosec capabilities, with managed secure hosting etc. People buy based on our experience. People come and visit the SOC, prospective customers" (I-17). For this interviewee, what were previously simply data management necessities

are now highly valued ‘infosec capabilities’. More importantly, as the earlier interviewee claimed, the close relationships that national telecoms companies cultivate with ‘security authorities’, and their ‘unique visibility’ at a country level are extremely valuable not just for marketing their cybersecurity services, but also for censorship and surveillance. I treat these two functions separately in the following sections.

9.3.1 Censorship

This section argues that telecoms companies elide commercial motivations for censorship within the larger national security priorities of their governments.

The central role of telecoms companies in censorship is due to the fact that, as ISPs, national telecoms companies have the power to control internet traffic over national borders. This power could be used to block access to the internet altogether, although there is only one instance of this occurring in this region: the internet shutdown in Egypt in January 2011. This shutdown was probably achieved through phone calls from a government agency to all major ISPs instructing them to stop services (although the ISP hosting the stock exchange remained online),[669] and reportedly cost the Egyptian economy around $110 million.[670] Blocking is thus a viable short-term strategy for governments in extreme circumstances and requires either control of either the ISPs themselves or their hardware. However, as the commercial cost of this blockage suggests, it is not a long-term solution, as economic pressures force states online again as soon as possible.

Many telecoms companies install surveillance and filtering equipment provided by the companies examined earlier in this thesis. As well as traffic management and analysis and the censorship of specific websites or content, telecoms companies often use this equipment to block Voice over IP (VOIP) services such as Skype, encrypted messaging, encrypted VOIP, and virtual private networks (VPNs). Although this blocking can be subtle, it occasionally has highly visible

[669] Larry Greenemeier, ‘How Was Egypt’s Internet Access Shut Off?’, Scientific American, 28 January 2011, https://perma.cc/T3LM-E88P.
[670] Parmy Olson, ‘Egypt’s Internet Blackout Cost More Than OECD Estimates’, Forbes, 3 February 2011, https://perma.cc/VP9Y-8HV9.

consequences. Most noticeably, Egypt accidentally interfered with national Google traffic when it blocked the encrypted messenger app Signal, and blocked VOIP and a wide range of news websites from 2016 onwards.[671] Unlike the 2011 shutdown, which required manual ISP cooperation in real time, this attempt was reported to originate from a centralised capability with the prior agreement of several ISPs.[672]

There is a clear national security rationale for the blocking of such services: it is more difficult (and in the early days of Skype, virtually impossible due to its peer-to-peer nature) to monitor and access call records from the (often US-based) technology companies who own VOIP software. Similarly, encrypted communications prevent even a national-level DPI-based system from reading individual data packets (although some DPI technologies, such as Blue Coat's ProxySG, claim to circumvent some forms of encryption). Consequently, in earlier chapters I framed this censorship activity in terms of national security motivations for governments on the one hand - in Egypt, a wide definition of terrorism used by the High Council for Cybersecurity – and commercial incentives for surveillance suppliers on the other.

However, there is a third motivation also at play: namely, the prevention of commercial competition to the national telecoms company. This motivation often is hidden behind security justifications, as was the case for mooted VOIP calling and VPN bans in the UAE in 2016. At the time, the TRA Director framed this ban in security terms, saying that "the security factor is important in the country. If we neglect it, online calling will impose risks."[673] However, in the same discussion other members of the Federal National Council complained about the high cost of calls, suggesting that it was profit as well as security that led Etisalat and Du to block competitors. These congruent incentives for telecoms companies filtered into legislation, including through a doubling of the fine for the use of a 'fraudulent IP address' (i.e. a VPN or compromised third-party device) in committing crime in the cybercrime law examined in Chapter 7.

[671] Staff Report, 'Infinite Eyes in the Network: Government Escalates Attack on Secure Communication', Mada Masr, 10 February 2017, https://perma.cc/8DJ5-SHD9.
[672] Staff Report, 'Egyptian Government Bypasses ISPs to Block Access to Websites: Telecommunications Ministry Source', Mada Masr, 21 June 2017, https://perma.cc/9WXV-DVFG.
[673] Haneen Dajani, 'UAE Telecoms Regulator Defends Decision to Block Snapchat Calling', The National, 12 April 2016, https://perma.cc/STL9-SLV5.

The overlap between commercial and security motivations for censorship is also present in other Gulf states. A US Embassy cable from Oman in 2009 assessed that VOIP blocking there was partly to prevent commercial competition to the national telecoms provider, although "the unstated and likely more significant rationale…may be that such services are out of reach of the listening ear of the government".[674] More widely, as a Bahraini interviewee explained for the GCC as a whole:

> There is a committee in the GCC which looks at VOIP – so far everyone in GCC has taken their own action, and done it differently. But Bahrain - which allows VOIP - is looking at the security aspect of VOIP for the OTT applications for the GCC committee. We are doing this work with a UK consultancy... We need them to look at all the risks of VOIP, and then work out what the residual risk is – that decides whether you should block it or not (I-55).

The risks of VOIP, for this interviewee, include not only the 'security aspect', but all the other risks as well, including the disruptive potential of such technologies for the national telecoms companies. This quotation suggests that telecoms companies hide their commercial motivations for censorship within the larger national security aims considered in earlier chapters. This is an example of the moral manoeuvre of elision, as it uses technical concepts to mask value differences between commercial and national security settings.

For an interviewee in the Qatari government, this elision was facilitated by a lack of clear direction from state agencies. When I asked about censorship in Qatar, the interviewee responded:

> We try to avoid the words 'monitoring' or 'censoring' in communications to the public. We don't have a well-established process to block websites, e.g. porn or gambling. We don't know who should take the decision on a site, and so far it has been ad hoc (I-53).

As well as strategic avoidance of the term censorship itself, this quotation highlights the perceived uncertainty for those involved in censorship around specific censorship decisions.[675] Their 'ad hoc' nature enables telecoms companies to not only *take* these decisions, but then to conceal their commercial motivations for censorship within wider national security rationales.

In sum, telecoms companies play a key role in censorship, occupying a position between surveillance suppliers and security services. This position allows them to elide national security and

[674] Wikileaks, 'US Cable: Skype Crackdown in Oman', 17 May 2013, https://perma.cc/XFS9-2WE7.
[675] Qatar still blocks critical political content. See Anon., 'Out of Sight, out of Mind? Blocking Doha News in Qatar', Journal of Middle Eastern Politics and Policy, 12 January 2017, https://perma.cc/UX6E-KMB2.

commercial risks of encrypted and alternative communications technologies. There is no norm-based alternative explanation for this moral manoeuvre, because telecoms companies are neither surveillance suppliers nor state actors.

9.3.2 Surveillance

As well as blocking a form of communication entirely, telecoms companies also enable security agencies' access to those communications. The same technologies can filter or intercept particular communications and so there are again three relevant actors involved in national surveillance systems: surveillance suppliers, the government, and the national telecoms company. This section argues that telecoms companies also elide commercial incentives for surveillance under the rubric of national security, and, like the surveillance reseller in the second section of this chapter, manipulate values in other ways outside the scope of norm-based accounts.

First, the legal framework mandating access to telecoms networks for national security reasons affects the surveillance decisions taken by telecoms companies both directly, as it creates a requirement to build systems for surveillance, and indirectly, as it creates commercial incentives for particular systems and practices of surveillance. While the UAE, Saudi Arabia, and Kuwait telecoms laws include general provisions for national security, Egypt, Oman, Qatar, and Bahrain all have specific articles concerning access to telecoms networks for national security organisations. The telecoms laws in Egypt (Article 64), Oman (Article 44) and Bahrain (Article 78) specify that such access should be maintained at the expense of the telecoms company themselves, while Qatari law (Article 60) states that the expenses incurred for the implementation of such systems be repaid by the state.[676] As such surveillance systems are expensive (in the millions of dollars), the legal structure

[676] Telecommunications Regulatory Authority (Oman), 'Royal Decree No. 30/2002 Telecommunications Regulatory Act' (Government of Oman, 2003); Telecoms Regulatory Authority (Bahrain), 'The Telecommunications Law of the Kingdom of Bahrain' (Government of Bahrain, 23 October 2002); ictQatar, 'Telecommunications Law - Decree Law No.34 of 2006' (Government of Qatar, 2006); National Telecom Regulatory Authority (Egypt), 'Telecommunication Regulation Law Law No.10 of 2003' (Arab Republic of Egypt, February 2003).

around surveillance access affects the commercial decisions and investment priorities of telecoms companies in surveillance software.

These investment priorities in turn shape the architecture of national surveillance systems. As one interviewee in the Bahrain Telecoms Regulation Agency explained:

> At the heart of communications between consumers and the outside world is a national security aspect – we facilitate the national security agency to have access to operators. We also make sure that operators meet their obligations technically to provide access to the national security agency… We are aiming to have a controlled centralised solution that we are in charge of, to enable this across providers (I-55).

In this 'controlled centralised solution', all telecoms companies would provide access to the security agencies, for example through key escrow with the regulator or a single national telecoms provider. The technical and hardware monopoly would be advantageous for economic reasons, as well as surveillance, illustrating the interplay between these incentives for telecoms companies.

Other states, such as Egypt, had historically adopted a more personalised approach. An Egyptian interviewee in the telecoms sector claimed that:

> 2003 saw the first law with cyber security in it – Law 10 in communications. But it had very general wording, and you can't use it to oblige certain organisations to do anything. It was used by national security agencies when they wanted to, especially for mobiles... But they are preparing a new law for 2017, which will be more specific. If there is a national security threat, then there will be a direct talk between the national security organisation and that business. (I-35).

This interviewee suggests that, despite the movements towards centralised censorship and surveillance in Egypt noted above, the primary means of access remained relationship-based. The legal framework facilitated these relationships, as the telecoms law could be used by security agencies 'when they wanted'. Crucially, in both cases economic reasons for either building a sophisticated solution or avoiding its implementation are concealed beneath a national security imperative: in Bahrain, as more efficient access to information, and in Egypt, as direct individual control of the relationship between the security services and telecoms companies. This echoes the elision of commercial incentives into national security requirements for filtering above, suggesting that telecoms companies elide their differing rationales in both cases.

The implementation of *national* rather than targeted surveillance solutions is also shaped by the economic priorities of telecoms companies, as illustrated in the case of Blackberry's encrypted messaging system in the UAE. In 2009, there was a controversial negotiation between RIM, the makers of Blackberry, and the UAE Telecoms Regulatory Authority (TRA) over access to encrypted communications. This focus on Blackberries was probably due in part to the strength of the encryption implementation (higher than competitors at the time), and also to the well-publicised use of Blackberries in the Mumbai terrorist attacks in December 2008.[677] Initially, a complete ban on Blackberry phones was reportedly threatened by the TRA.[678] However, a complete ban would create significant costs for companies using Blackberry and the UAE's international reputation as a regional commercial hub.[679]

Instead, the UAE national telecoms company, Etisalat, installed surveillance software from the US company SS8 on Blackberry phones in July 2009.[680] The software, described as a 'performance update' and prompted by a text from Etisalat, enabled information from the phone to be transmitted to Etisalat without the user's knowledge. The spyware was removed by RIM soon after it was detected, and Etisalat claimed it was a 'technical fault'. The installation of device-based surveillance software by Etisalat was probably either condoned or instructed by the government. If so, it could be read as an early attempt by the government to obtain access to such phones rather than resorting to a complete ban. However, following the involvement of Etisalat in the UAE government's attempts to gain access to Blackberry devices, RIM reportedly provided access to Blackberry data for the UAE government in April 2011,[681] as they did for Saudi Arabia and Kuwait in 2010.[682] This evolution of Blackberry surveillance in the UAE demonstrates the gradual evolution

[677] Emily Wax, 'Mumbai Attackers Made Sophisticated Use of Technology', *Washington Post*, 3 December 2008, https://perma.cc/SH9U-BT7M.
[678] Richard Wray, 'UAE BlackBerry Ban Set to Spread throughout Gulf States', *The Guardian*, 2 August 2010, https://perma.cc/KFA2-NHRN.
[679] For Blackberry, this is a worldwide issue. Staff Report, 'India Is "ready to Use" Blackberry Message Intercept System', *BBC News*, 11 July 2013, https://perma.cc/MJ8K-2R3F.
[680] Ben Thompson, 'UAE Blackberry Update Was Spyware', BBC News, 21 July 2009, https://perma.cc/97UP-3APN.
[681] Josh Halliday, 'UAE to Tighten BlackBerry Restrictions', *The Guardian*, 18 April 2011, https://perma.cc/PH46-HF32.
[682] Souhail Karam and Diana Elias, 'BlackBerry in Bid to Address Saudi Security Concerns', *Reuters*, 8 August 2010, https://perma.cc/K9N7-J2BB.

of surveillance architectures towards centralised national solutions rather than device-based surveillance that are less efficient and more difficult to maintain *for the telecoms companies*.[683] As such, the economic priorities of national telecoms companies play a key role in these negotiations, both as interested parties and as the means through which potential surveillance solutions can be tested.

Finally, telecoms companies also engage in the reinterpretation of human rights values in a similar way to surveillance suppliers analysed in the previous chapter. In 2013 a security researcher claimed to have been approached by Mobily, a telecoms company in Saudi Arabia. Mobily reportedly asked for his assistance in the interception of social media apps including Whatsapp and Twitter.[684] The request, from their "Network and Information Security Department", indicated that it came from the Saudi government, saying that "we are working in defining a way to deal with all such requirements from regulator and it is not only for Whatsapp, it is for whatsapp, line, viber, twitter etc..". This researcher stated that:

> One of the design documents that they volunteered specifically called out compelling a CA [certificate authority] in the jurisdiction of the UAE or Saudi Arabia to produce SSL [encryption] certificates that they could use for interception. A considerable portion of the document was also dedicated to a discussion of purchasing SSL vulnerabilities or other exploits as possibilities.[685]

The inclusion of the UAE as well as Saudi Arabia is interesting, suggesting linked surveillance systems in the two states. This quotation also highlights an alternative strategy for telecoms companies instead of purchasing surveillance capabilities from external providers, instead recruiting individuals as contractors to build a similar system internally. When Mobily's request for assistance was rejected by the researcher, citing "privacy reasons", their response was as follows:

> I have same thoughts like you freedom and respecting privacy, actually Saudi has a big terrorist problem and they are misusing these services for spreading terrorism and contacting and spreading their cause that's why I took this and I seek your help. If you are not interested than maybe you are on indirectly helping those who curb the freedom with their brutal activities.[686]

[683] Dark Matter may be involved in maintaining this solution, as they opened a Toronto-based research division not far from Blackberry headquarters in 2016.
[684] Moxie Marlinspike, 'A Saudi Arabia Telecom's Surveillance Pitch', 13 May 2013, https://perma.cc/GT39-6JL5.
[685] Marlinspike.
[686] Marlinspike.

Here the telecoms company representative altered human rights values by assimilating them into the broad definition of national security used in Saudi Arabia. They then used these values to attempt to persuade the researcher to cooperate, claiming that the alternative to surveillance is 'curbing freedom'. This goes beyond the moral manoeuvre of elision considered so far in this chapter, incorporating several of the themes explored earlier in this thesis.

Overall, this section has argued that telecoms companies play a key role in both censorship and surveillance, between technology suppliers and government organisations. Telecoms companies alter the values in cybersecurity in ways not addressed by norm-based alternatives, by eliding their commercial motivations into wider national security concerns, and manipulating human rights values in a similar manner to surveillance suppliers.

***

This chapter has examined the moral manoeuvre of elision. It began by showing how specialised cybersecurity companies created cybersecurity knowledge in the region. It then investigated portable concepts within this knowledge, including network visibility and insider threats, arguing that these concepts elide the difference between commercial and national security environments in cybersecurity by facilitating both national surveillance and protective organisational measures. Finally, it explored the role of telecoms companies in censorship and surveillance, arguing that they also elide commercial and national security values in their unique role between governments and surveillance suppliers. Overall, this chapter has demonstrated that actors outside the scope of cyber norms perform moral manoeuvres by renegotiating both values and technical concepts in cybersecurity, extending the theoretical framework of this thesis beyond norm-based alternatives.

Chapter 10. Conclusion

Cybersecurity in Egypt and the Gulf states continues to change, reflecting the myriad flows of information with which it is concerned. The Gulf crisis in June 2017, marking the end of the period studied by this thesis, illustrates this fluctuating terrain well. The immediate pretext for the ostracisation of Qatar by Egypt, Saudi Arabia, the UAE and Bahrain was genuine footage of the Qatari emir Sheikh Tamim Al-Thani that appeared on the website of Qatar News Agency (QNA) just after midnight on 24 May 2017, but with fabricated text that portrayed him as expressing support for Iran and the Muslim Brotherhood. Following its publication, news agencies in the quartet states picked up the story almost immediately, suggesting that they were prepared for its release. At least three dailies in Saudi Arabia and one in UAE led with it in their morning headlines on 24 May.[687]

Qatar's investigation, supported by the FBI and the UK National Crime Agency, concluded that the appearance of the video was the result of a cyber operation against QNA.[688] Sources told the international press that the UAE or Saudi Arabia hired Russian contractors to conduct the operation. The Washington Post reported unnamed US national security officials as saying that the intrusion was carried out by contractors working for the UAE.[689] Separately, The New York Times cited anonymous US and Qatari officials as blaming Russian hackers for hire, and the Guardian reported observers' suggestions that the UAE or Saudi Arabia had commissioned the hackers.[690] In addition, on 20 June the Qatari attorney-general claimed Qatar had evidence that iPhones from the quartet countries were used in the operation.[691] While the Qatar crisis had many long term causes, the use of

---

[687] MEMRI, 'Uproar In The Gulf Following Alleged Statements By Qatari Emir Condemning Gulf States, Praising Iran, Hizbullah, Muslim Brotherhood And Hamas', Middle East Media Research Institute Inquiry and Analysis Series No.1315, 25 May 2017, https://perma.cc/SUK8-YHDK.

[688] Staff Report, 'Qatar Reveals Preliminary Results of QNA Hacking Probe', Al-Jazeera, 7 June 2017, https://perma.cc/6VVW-EGFC.

[689] Karen DeYoung and Ellen Nakashima, 'UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials', *Washington Post*, 16 July 2017, https://perma.cc/3A5U-LCTR.

[690] David D. Kirkpatrick and Sheera Frenkel, 'Hacking in Qatar Highlights a Shift Toward Espionage-for-Hire', *The New York Times*, 8 June 2017, https://perma.cc/4FBM-R24K; Patrick Wintour, 'Russian Hackers to Blame for Sparking Qatar Crisis, FBI Inquiry Finds', *The Guardian*, 7 June 2017, https://perma.cc/3CFY-ZQ6D.

[691] Julian Borger, 'US Rebukes Saudi Arabia over Qatar Embargo in Reversal after Trump Comments', *The Guardian*, 20 June 2017, https://perma.cc/PW3P-6RFX.

cyber means to initiate the complete ostracization of a neighbouring state was a new development in the region and in the politics of cybersecurity more generally.

Social media was also used strategically for disinformation during the Qatar crisis. The sites 'Qatarileaks' and ‘The Qatar Insider’ were created at around the same time, carrying anti-Qatar propaganda. Just before the ostracisation, but after the QNA incident, an unknown individual offered the private emails of the influential UAE ambassador to Washington, Yusuf Al-Otaiba, to several US news outlets.[692] These emails indicated that Otaiba had significant influence with several think tanks and government figures including the President’s advisor and son-in-law Jared Kushner, as well as a lavish lifestyle and anti-Qatar posture. Their publication was probably a Qatari response to the earlier cyber operation. Both sides also recognised the importance of social media in shaping public opinion in their favour.[693] Throughout August, a popular Saudi figure on Twitter misleadingly interpreted the quantity of anti-Qatar hashtags as demonstrating popular support against the ruling Al-Thani family in Qatar, even though most of those accounts were located in Saudi Arabia.[694] In December, the popular 'Saudi citizen' account was hijacked, tweeting pro-Al Thani comments.[695] The fervent nationalism inculcated on both sides by the Qatar crisis has led to new understandings of the effects and limits of digital technologies, and of cybersecurity itself.

This brief account of the Qatar crisis suggests that cybersecurity continues to be a widely contested and highly relevant aspect of politics in Egypt and the Gulf states, contributing to drastic changes in the political landscape of the region. More generally, the theoretical lens employed by this thesis can also be used to understand moral dynamics elsewhere in international politics. This chapter concludes the thesis by exploring some of these avenues, after first summarising the argument and contributions of the thesis, its policy implications, and limitations.

---

[692] Akbar Shahid Ahmed, ‘Someone Is Using These Leaked Emails To Embarrass Washington’s Most Powerful Ambassador’, HuffPost UK, 3 June 2017, https://perma.cc/97VG-J3ZR.
[693] Bahrain Watch, ‘Uncovering a Twitter Bot Army Mobilised Against Al Jazeera’, Amantech by Bahrain Watch, Digital Defenders Partnership, 24 July 2017, https://perma.cc/39MC-W75G.
[694] Marc Owen Jones, ‘Saudi Royal Court Advisor Saud Al-Qahtani Is Using Bad Science to Inflame Tensions with Qatar’, Marc Owen Jones, 23 August 2017, https://perma.cc/Y4X5-WSDS.
[695] ʿAbdallah Al-Barqawi, ‘ʿajil… “Suqur Al-Qatar” Takhtariqu “Hisab Al-Muwatin” [Breaking… “Qatari Falcons” Hack “the Citizen’s Account”]’, Sabq, 2 January 2018, https://perma.cc/U98N-ALN4.

10.1 Argument and contributions

This thesis has answered the research question: how can we explain the nature of cybersecurity in Egypt and the Gulf states? This thesis has argued that cybersecurity is built on an ambiguous professional discourse that combines several referents – i.e. *who* cybersecurity protects against *what* – into a generic 'organisational' cluster of values in cybersecurity. Various actors in Egypt and the Gulf states use this ambiguous professional discourse to perform what I call *moral manoeuvres*: the alteration of values and technical claims and the renegotiation of the relationship between the two. These actors are either *invested*, meaning that they seek to promote a particular value or cluster of values, or they are *agnostic*, seeking ends that do not include a commitment to any specific values. Each moral manoeuvre takes cybersecurity in a different direction, and their *co-existence* is the key insight of this thesis. Thus, the nature of cybersecurity in Egypt and the Gulf states is syncretism, improvisation, and contradiction, arising from the mobilisation of an ambiguous expert discourse by various actors for very different purposes.

This thesis began by situating its empirical research within the broader cybersecurity literature in IR. It highlighted the contribution of critical and constructivist theories to cybersecurity studies in IR, especially in their understanding of cybersecurity as contingently constructed for specific purposes. The thesis then placed the concept of moral manoeuvres directly in conversation with literature on 'cyber norms'. It suggested that despite a clear political motivation to promote cyber norms, such norms have had little success in practice. Furthermore, cyber norms have suffered from similar problems identified by norm studies more broadly: they are interpreted differently by their advocates and opponents and used or ignored by various parties at different times. Consequently, although values play a key part in cybersecurity, an analysis in terms of norms leaves much to be explained.

Instead, I used the distinction between invested and agnostic actors to specify four separate moral manoeuvres. First, actors invested in a particular value or cluster of values can seek to reframe their value preferences to fit the discourse, which I call *alignment*. Second, invested actors can do the opposite and seek to expand the discourse to fit their value preferences, which I call

appropriation. Third, actors who are agnostic between different values or clusters of values can seek to exploit the contradictions between those values within the discourse, which I call *manipulation*. Fourth, agnostic actors could also do the opposite and minimise these contradictions, which I call *elision*.

The main empirical body of the thesis detailed these four moral manoeuvres. First, NGOs defined cybersecurity as an issue of government threats to individual rights rather than threats from a range of malicious actors to organisations. These actors *aligned* a rights-based conception of cybersecurity with the dominant organisational conception, contributing to debates over legitimate cybersecurity practices.

Second, government agencies, especially ministries of interior and state security agencies, *appropriated* organisational values under an expansive concept of national security. These actors saw cybersecurity technologies as national-level intelligence capabilities, and defined cybercrimes as political speech online rather than economic threats. This appropriation – using both discursive and more concrete forms of power – inverted the rights-based views of NGOs, casting rights activists as cybersecurity threats to the state rather than vice versa.

Third, surveillance suppliers to the governments of Egypt and the Gulf states *manipulated* both organisational and human rights values to maintain sales of surveillance technologies. These actors used both sophisticated technical claims about their capacity to monitor surveillance software once sold and new institutional structures to place the 'misuse' of such technologies within a broader risk framework. Although exporting states deployed different mechanisms to private companies, both manoeuvred between national security and human rights to retain flexibility in their sales decisions.

Fourth, the wider cybersecurity industry *elided* value differences between commercial and national security environments, using portable technical concepts to facilitate the sale of cybersecurity technologies in both settings. Specialised cybersecurity companies and their local resellers used their core role in the production of cybersecurity knowledge to transfer technologies and practices between these two environments. Telecoms companies also elided their commercial incentives for censorship and surveillance behind national security requirements.

Together, these four moral manoeuvres constituted the key dimensions along which cybersecurity took shape in Egypt and the Gulf states. Their simultaneous performance, improvised creatively in the context of – but not always as a response to – other invested and agnostic actors, moulded the contours of the cybersecurity landscape, preserving and even amplifying the contradictions and ambiguities present in the original professional discourse. The practical consequences of these moral manoeuvres were extensive, including the creation of new international agreements, new laws and regulations at both domestic and regional levels, new public and private structures for accountability, and new technical knowledges.

Through its development and application of the concept of moral manoeuvres, this thesis has made three original contributions to IR. First, it has provided a more detailed understanding of the moral dynamics of cybersecurity than that available through critical security studies, showing how actors actively redirect the ambiguous cybersecurity discourse identified by critical cybersecurity scholars in multiple dimensions, rather than reciprocal securitisations and counter-securitisations. Second, this thesis has put forward new data on an underexamined issue in a previously unstudied region to demonstrate the utility of the concept of moral manoeuvres. This data, including sensitive interviews, participant observation in professional conferences, and the discourse analysis of laws and regulations, technical reports and leaked documents, is useful to both cybersecurity and Middle East studies. The third contribution of this thesis is to the literature on cyber norms. Many scholars have noticed how the performative and interpretative nature of values and norms has undermined relatively mechanical models of norm adoption in the international system. This thesis argued that the concept of norm should not necessarily be diluted to take account of the fluid and often instrumental quality of values in cybersecurity, as these dynamics can instead be theorised as moral manoeuvres.

10.2 Policy implications

The argument of this thesis is relevant not only for IR theory, but also to policymakers, cybersecurity practitioners and individual users of digital technologies. In this section I relate the

findings of this thesis to policy recommendations on cyber norms and the cybersecurity 'skills gap', primarily issued in US and European think-tanks, governments and supranational institutions.

First, this thesis suggests that cyber norms are the beginning rather than the end of contest and competition over values in cybersecurity. The empirical research of this thesis shows that international agreements and conventions are not only provisional but are continually liable to fundamental change, because actor-groups perform moral manoeuvres rearticulating the values and technical claims underlying these normative prescriptions. Consequently, more attention should be paid to what comes *after* the establishment of cyber norms, not just in terms of compliance but also in terms of reinterpretation and rearticulation of the scope and purpose of cybersecurity itself.

For example, as Chapter 8 demonstrated, the Wassenaar amendment was incorporated by both surveillance suppliers and exporting states into a moral manoeuvre that manipulated both national security and human rights values to maintain prior sales practices. The policy implication of this finding is a requirement for increased transparency around ethical decisions made by exporting states and companies. This could include the publication of instances, even anonymised, where export licences are revised and resubmitted (rather than simply the number of licences granted), and where companies cease cooperation or change their contracts based on export stipulations. This call for transparency can be extended to states in which many rights violations take place, asking them to release details of their investigations into such violations if they are conducted.

Another example is the Budapest Convention on Cybercrime, championed by many policymakers in the US and Europe who seek a means to prosecute malicious cyber actors outside their jurisdictions. However, as demonstrated in Chapter 7, the Budapest Convention was incorporated into the moral manoeuvre of appropriation, where cybercrime is expanded to target political speech online rather than economic threats. The policy challenge for organisations implementing or advising on cybercrime legislation is to anticipate how emerging issues such as disinformation and opinion shaping might enable further appropriation of cybersecurity concepts and their use against political opposition.

The second set of policy implications are around cybersecurity expertise. Cybersecurity experts are in great demand in many regions of the world. This demand is often characterised as a

cybersecurity "skills gap", where "cyberattacks are growing, but the talent pool of defenders is not keeping pace".[696] Policy responses to this skills gap focus on adapting curricula, creating competitions to demonstrate technical skill, and training staff on-the-job.[697] However, these policies are hampered by the unclear content of cybersecurity expertise. Cybersecurity professionals appear to require a vast range of skills from communications, compliance, data analytics and organisational psychology, as well as information technology.[698]

The approach to expertise taken in this thesis means we should rethink concerns over a cybersecurity "skills gap". The skills gap stems from a supposed mismatch between the level of risk and the number of cybersecurity experts. However, this level of risk is itself the *result* of a successful performance by those experts. Cybersecurity risk expands as more knowledge pools are brought to bear on cybersecurity, with ever more additions to the "attack surface". As long as cybersecurity continues to accrue social and political capital, this proliferation of relevant domains will continue, and the required repertoire of the "sufficiently skilled" cybersecurity professional will continue to expand. A gap is the wrong metaphor for this process, as it obscures the connection between expanding expert performance and increasing risk.

Finally, this thesis also has policy implications at an individual level. First, and most obviously, individuals should take responsibility for protecting themselves and their data from cybersecurity threats, especially if they are in particular at-risk groups. There are good resources available for individuals to understand these threats and take easy steps to mitigate them.[699] Second, individuals can also personally reflect on the cybersecurity values around them using the concept of moral manoeuvres outlined in this thesis. Where they are involved in the alteration of values or redefinition of technical concepts in ways that are traced in the empirical body of this thesis, individuals can use the concept of moral manoeuvres to *recognise* this phenomenon as it happens.

[696] ISACA, '2016 Cybersecurity Skills Gap' (Cybersecurity Nexus, January 2016), https://perma.cc/3BZV-K2LY.
[697] Rebecca Vogel, 'Closing the Cybersecurity Skills Gap', *Salus Journal* 4, no. 2 (2016): 32–46.
[698] John Pironti, 'The Changing Role of Security Professionals', Infosecurity Magazine, 15 January 2013, https://perma.cc/88PD-6HCU.
[699] For example, https://ssd.eff.org/en, https://securityplanner.org/

By doing so, individuals could seize such moments of fluidity to rearticulate cybersecurity differently, to create space for new conceptions of cybersecurity and resist dominant interpretations.

10.3 Limitations

This section examines the limitations of the empirical research conducted for this thesis. All research designs have limitations and constraints created by their philosophical premises, methodological directions, and practical requirements. Consequently, although the research design chosen was most suitable for the research question asked by this thesis, especially as the first IR study of an understudied region in an understudied issue, it nonetheless included unavoidable limitations. I detail three methodological limitations, corresponding to the three main methods used in this thesis: discourse analysis, interviews, and participant observation, and then a specific limitation due to the topic of cybersecurity. These limitations do not invalidate the conclusions of this thesis: rather, they create opportunities for future work.

First, the discourse analysis conducted in this thesis was limited in terms of the corpus selected and its analysis. Future research could conduct a more systematic study of speeches and other pronouncements on cybersecurity by national governments in Egypt and the Gulf states, rather than focusing on cybersecurity strategies and laws. Including this corpus would provide a richer basis for the analysis of appropriation in Chapter 7. This thesis also conducted predominantly textual rather than multimodal discourse analysis. Security studies suggests that images securitise issues in a wide variety of ways,[700] while cybersecurity scholars have argued that visualisation is a key aspect of creating cybersecurity worldviews.[701] I collected a large set of images used in cybersecurity conferences and cybersecurity professional documents, and a different research design would include a semiotic analysis of these images.

[700] Roland Bleiker, 'The Aesthetic Turn in International Political Theory', *Millennium* 30, no. 3 (1 December 2001): 509–33; Lene Hansen, 'Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis*', *European Journal of International Relations* 17, no. 1 (1 March 2011): 51–74.
[701] Peter Hall, Claude Heath, and Lizzie Coles-Kemp, 'Critical Visualization: A Case for Rethinking How We Visualize Risk and Security', *Journal of Cybersecurity* 1, no. 1 (1 September 2015): 93–108.

The second method used in this thesis was interviews, with limitations in both their selection and conduct. A larger number of interviews would enable the investigation of broader patterns and provide greater empirical weight to the material used in the thesis. The interview process was limited both in terms of language (interviews were all conducted in English), and because it was semi-structured. While this allowed interviewees space to explore their personal understanding of cybersecurity, it made it difficult to explicitly address the interviewee's conception of the relevant values for cybersecurity at the outset of the interview. A structured approach to interviews may provide a different kind of empirical data to test the view of moral manoeuvres presented in this thesis. Finally, the scope of interviews was restricted to cybersecurity experts. Other interview strategies could include activists or hackers in the region without an emphasis on expertise, adding to excellent work on hacker communities in Europe.[702]

The third method used in this thesis was participant observation, which was limited by the transient conference sites chosen. Other scholars have attempted to access a professional cybersecurity environment using long-term participant observation in SOCs (Security Operations Centres). These scholars have identified several new aspects of cybersecurity expert performance, including detailed information about workflows and reflections on their perceived status.[703] While the conference participant observation in this thesis successfully accessed the professional community on a larger scale than an individual SOC, I was unable to observe the day-to-day work of cybersecurity professionals in this region. Following a particular organisation or a smaller group of individuals for a more sustained period may provide a contrasting insight into cybersecurity professional practices.

Reflexive analysis of my own epistemological, moral, and other commitments is an important aspect of participant observation. In this analysis, I attempted to avoid two related pitfalls. The first is an assumption of superiority: that the interpretation offered here is somehow truer, better,

[702] Leonie Maria Tanczer, 'Hacktivism and the Male-Only Stereotype', *New Media & Society*, 14 January 2015.
[703] Sathya Chandran Sundaramurthy et al., 'A Tale of Three Security Operation Centers', in *Proceedings of the 2014 ACM Workshop on Security Information Workers*, SIW '14 (New York, NY, USA: ACM, 2014), 43–50; S. C. Sundaramurthy et al., 'An Anthropological Approach to Studying CSIRTs', *IEEE Security Privacy* 12, no. 5 (September 2014): 52–60.

or more accurate than an 'inside' interpretation. The second is a refusal of symmetry. As Latour notes, ethnography often reserved for those who are assumed not to be 'Modern' and it is not applied symmetrically to Modern practices.[704] To counter these pitfalls, the analysis above is an intervention in a conversation not only with other academics, but with conference participants as well, to be judged and critiqued on both levels. Furthermore, cybersecurity professionals, as highly qualified graduates of advanced engineering and scientific courses, are as Modern in Latour's sense, if not more so, than any social scientist who works with and alongside them. Consequently, my methods and conclusion are as open to critique by them as much as their practices are questioned here.

As well as these limitations stemming from research design, there is a more specific limitation to empirical research on cybersecurity in Egypt and the Gulf states. One of the underlying themes of this thesis is that cybersecurity is an inclusive issue area, involving a wide range of actors. This assisted my empirical research as it facilitated my access to areas that may not be available to researchers without the 'cybersecurity' label. However, it also means that the identity of a researcher is a useful one to adopt for many cybersecurity actors who are not in fact researchers, with two striking examples.

The first example involves phishing emails: emails that purport to be from a legitimate contact that either convince the target to provide credentials or enable the introduction of malware to the target network. Some phishing emails sent by cybersecurity threat actors look very similar to the emails I sent asking for interviews. For example, this is a phishing email sent to a journalist working on technology and human rights in the Gulf:[705]

[704] Bruno Latour, *On the Modern Cult of the Factish Gods* (Durham NC; London: Duke University Press Books, 2010).
[705] Marczak and Scott-Railton, 'Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents'.

> From: andrew.dwight389@outlook.com
> Subject: FW: Correspondence RequestGreetings Mr. Donaghy,
>
> I have been trying to reach you for comment and I am hoping that this e-mail reaches the intended recipient. My name is Andrew Dwight and I am currently writing a book about my experiences in the Middle East. My focus is on human factors and rights issues in seemingly non-authoritarian regimes (that are, in reality, anything but). I was hoping that I might correspond with you and reference some of your work, specifically this piece ([MALICIOUS LINK]), for the book. I'm quite impressed with the way you articulate this complex issue for the masses, and hope to have a similar impact with my book.
>
> Happy New Year,
>
> Andrew

This email was sent by a group named Stealth Falcon, likely associated with the UAE government (detailed in Chapter 6). The link in the email above was intended to install malware on the device of the targeted individual. Many of my email approaches to cybersecurity professionals looked similar, as they included a brief summary of the topic, a request for discussion, and a reason for contacting that particular person (although I did not include any links). This demonstrates a limitation of interview-based research on cybersecurity in Egypt and the Gulf; namely, that potential interviewees are already suspicious of researcher profiles like mine. Consequently, these emails were rarely successful, and I relied on face-to-face meetings and referrals to obtain interviews.

The second example is a set of documentaries by the UK channel ITV aired in 2016, which presented undercover footage of Saudi Arabia including executions, floggings, and extensive poverty.[706] This series relied on activist networks in Saudi Arabia and undercover filming. The journalists who entered Saudi Arabia to film for this documentary did so using the cover of a UK-based cybersecurity company, and they even signed up to a cybersecurity conference in Saudi Arabia to obtain a visa. This journalistic methodology closely resembled my research design, as I also attended cybersecurity conferences in Saudi Arabia and across the region. Although this deception is clearly outside the ethical boundaries of my research – my attendance at cybersecurity conferences was a core part of the research, rather than a front for another purpose – it meant that cybersecurity

[706] ITV, 'Saudi Arabia Uncovered - Exposure Episode 1', Press Centre, 9 March 2016, https://perma.cc/68PL-XQBP.

conferences were not only populated by the cybersecurity professional community, but were also targeted as a lever for access to Saudi Arabia by individuals with very different purposes.

10.4 Further work

This section details further work on the concept of moral manoeuvres in three directions in addition to the alternative research designs above: first, on cybersecurity in Egypt and the Gulf states; second, on cybersecurity more widely; and third, on IR issues outside cybersecurity. Each direction is suggested by the theoretical logic of this thesis, as it would extend or challenge the concept of moral manoeuvres in different ways.

Further work on cybersecurity in Egypt and the Gulf states could extend the empirical research of this thesis to other actors such as large multinational technology companies like Google, Apple, and Microsoft, or 'platform' companies like Twitter or Facebook. Although these companies do not have the same relationship to human rights values as NGOs, they do not have the same national security connections as surveillance suppliers, specialist cybersecurity companies, or telecoms monopolies. Investigating whether and how these companies perform moral manoeuvres in the region would be a logical extension of the theoretical approach taken here. It could also examine 'compound' moral manoeuvres, combining the four moral manoeuvres in this thesis.

Further work could also examine other aspects of cybersecurity expertise in this region. One route to take would be to emphasise gender as a structuring device for the cybersecurity profession itself. I treated the gender assumptions behind cybersecurity technologies, organisations, and individuals briefly in Chapter 4, recognising that further work is required. Another might be to take a postcolonial approach to cybersecurity expertise. An analysis of cybersecurity experts in these terms would investigate the national and ethnic hierarchies behind apparently technological and organisational concepts of cybersecurity, and the ways in which colonial or semi-colonial legacies shape cybersecurity more broadly.

Looking outside Egypt and the Gulf states, further work could ascertain whether the four moral manoeuvres identified in this thesis are present in other regions within the issue area of

cybersecurity. Specifically, I argued that Egypt and the Gulf states share a hybrid approach to cybersecurity governance between the two poles of a multistakeholder and cyber sovereignty model, due to their close security ties to the US and Europe *and* their support of the ITU with other authoritarian states. Further studies could take a strategy of contrast, exploring whether moral manoeuvres are also performed in regions that fit more clearly within the bipolar model, such as China. It could also take a strategy of similarity, investigating whether actors in other hybrid states such as Brazil, India, or Kenya also perform the moral manoeuvres identified here.

Finally, the concept of moral manoeuvres could be deployed elsewhere in IR where there is an ambiguous and influential expert discourse. Consider, for example, climate change. The significant problems and contradictions in climate change politics stem not just from disagreements about how best to act, or what rules to follow, but from very different moral judgements of actors (states, companies, individuals) and objects (materials, territories, species, ecosystems, economies).[707] Climate change also incorporates several value clusters, including human rights.[708] However, value judgements in climate change are also dependent on an ambiguous professional discourse, depending on technical claims about historic carbon emissions, consequences of industrial development, damage to species and habitats, and the operation of offsetting schemes.[709] Climate change, therefore, would be a suitable alternative issue area in which to assess the wider applicability of the concept of moral manoeuvres.

Another potential issue area in which to examine moral manoeuvres is artificial intelligence (AI). AI fundamentally challenges dominant value structures in IR, as it involves human relationships with unusual actors – artificially intelligent machines – that raise a range of moral issues regarding fairness, justice, exploitation, compassion and so on. In AI, policy work recognises that satisfactory AI control in morally challenging situations, such as cars or weapons, is difficult even

[707] Peter Newell, *Climate Capitalism: Global Warming And The Transformation Of The Global Economy* (London: Cambridge University Press, 2010); Mitchell, *Rule of Experts*.
[708] Timothy W. Luke, *Ecocritique: Contesting the Politics of Nature, Economy, and Culture* (Minneapolis: University of Minnesota Press, 1997).
[709] Diana M. Liverman, 'Conventions of Climate Change: Constructions of Danger and the Dispossession of the Atmosphere', *Journal of Historical Geography* 35, no. 2 (1 April 2009): 279–96.

within standard moral theories.[710] However, it understates the depth of expert contest over the design of AI and its place in society. It also bypasses the larger issue that AI is likely to change accepted modes of moral decision-making themselves. If AI is used to make value judgements on a massive scale *about* other algorithmic systems, as with social media content, then value judgement itself, like other AI-enhanced human faculties, will become more discrete and rule-bound (although not less complex). Consequently, the examination of moral manoeuvres in AI would provide an important extension to the focus on cybersecurity here.

In conclusion, the concept of moral manoeuvres provides an original contribution to existing IR theories, especially on international norms. The fourfold typology of moral manoeuvres proposed here could be extended within the region to include gender and postcolonial legacies, applied to other hybrid regions in cybersecurity, or deployed in other issue areas where there is an ambiguous and influential expert discourse and multiple value positions, such as AI and climate change. There are many other areas of IR with similar features, such as development, finance, and food production, and so the concept of moral manoeuvres has a wide range of potential applications. One of the fundamental questions in IR is the place of values in a world infused with myriad forms of power. This thesis offers a new perspective on this profound and persistent question through the concept of moral manoeuvres. By piercing the carapace that envelops all forms of expertise, especially around ubiquitous digital technologies, it has tracked the ambiguities and tensions in values and facts that constantly diffuse and coalesce beneath the surface of international politics.

[710] UK House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (Report of Session 2017–19, 16 April 2018).

Bibliography

The bibliography contains all works cited in this thesis, in the following sections:

Academic works:	Articles and book chapters Books
Non-academic works:	Arabic sources Official sources (English) Non-official sources (English)
Archives:	Citizen Lab reports Wikileaks

Articles and Book Chapters

AbuSaad, Belal, Fahad Saeed, Khaled Alghathbar, and Bilal Khan. 'Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes, and Lessons Learned'. *Australian Information Security Management Conference*, 1 January 2011.

Acharya, Amitav. 'How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism'. *International Organization* 58, no. 2 (2004): 239–75.

Allagui, Ilhem. 'Internet in the Middle East: An Asymmetrical Model of Development'. *Internet Histories* 1, no. 1–2 (2 January 2017): 97–105.

Alshitri, Khalid I., and Abdulmohsen N. Abanumy. 'Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia'. In *2014 International Conference on Information Science Applications (ICISA)*, 1–4, 2014.

Amoore, Louise. 'Security and the Incalculable'. *Security Dialogue* 45, no. 5 (1 October 2014): 423–39.

———. 'Vigilant Visualities: The Watchful Politics of the War on Terror'. *Security Dialogue* 38, no. 2 (1 June 2007): 215–32.

Anderson, Jon W. 'Is Informationalization Good for the Middle East?' *Arab Media & Society* Summer, no. 18 (12 June 2013).

———. 'Producers and Middle East Internet Technology: Getting beyond "Impacts"'. *Middle East Journal* 54, no. 3 (2000): 419–31.

Aradau, Claudia. 'Security That Matters: Critical Infrastructure and Objects of Protection'. *Security Dialogue* 41, no. 5 (1 October 2010): 491–514.

Aradau, Claudia, and Rens Van Munster. 'Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future'. *European Journal of International Relations* 13, no. 1 (1 March 2007): 89–115.

Arquilla, John, and David Ronfeldt. 'The Advent of Netwar: Analytic Background'. *Studies in Conflict & Terrorism* 22, no. 3 (1 August 1999): 193–206.

Baldwin, David A. 'The Concept of Security'. *Review of International Studies* 23, no. 1 (January 1997): 5–26.

Balzacq, Thierry, and Myriam Dunn Cavelty. 'A Theory of Actor-Network for Cyber-Security'. *European Journal of International Security* 1, no. 02 (July 2016): 176–198.

Barkawi, Tarak, and Mark Laffey. 'The Postcolonial Moment in Security Studies'. *Review of International Studies* 32, no. 2 (April 2006): 329–52.

Barnard-Wills, David, and Debi Ashenden. 'Securing Virtual Space Cyber War, Cyber Terror, and Risk'. *Space and Culture* 15, no. 2 (1 May 2012): 110–23.

Barnett, Michael. 'Evolution without Progress? Humanitarianism in a World of Hurt'. *International Organization* 63, no. 4 (2009): 621–63.

Barnett, Michael, and F. Gregory III Gause. 'Caravans in Opposite Directions: Society, State and the

Development of a Community in the GCC'. In *Security Communities*, edited by Emmanuel Adler and Michael Barnett, 161–97. Cambridge, UK; New York: Cambridge University Press, 2008.
Barry, Andrew. 'The Translation Zone: Between Actor-Network Theory and International Relations'. *Millennium - Journal of International Studies* 41, no. 3 (1 June 2013): 413–29.
Bassiouni, Mahmoud Cherif. 'Egypt's Unfinished Revolution'. In *Civil Resistance in the Arab Spring: Triumphs and Disasters*, edited by Adam Roberts, Michael J. Willis, Rory McCarthy, and Timothy Garton Ash, 53–87. Oxford: Oxford University Press, 2016.
Bendrath, Ralf. 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection'. *Information&Security* 7 (2001): 80–103.
Betz, David J., and Tim Stevens. 'Analogical Reasoning and Cyber Security'. *Security Dialogue* 44, no. 2 (1 April 2013): 147–64.
Bigo, Didier. 'Globalized (in)Security: The Field and the Ban-Opticon'. In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 10–49. London; New York: Routledge, 2008.
———. 'Security and Immigration: Toward a Critique of the Governmentality of Unease'. *Alternatives* 27, no. 1 (1 February 2002): 63–92.
Bleiker, Roland. 'The Aesthetic Turn in International Political Theory'. *Millennium* 30, no. 3 (1 December 2001): 509–33.
Bloomfield, Alan. 'Norm Antipreneurs and Theorising Resistance to Normative Change'. *Review of International Studies* 42, no. 2 (April 2016): 310–33.
Boulanin, Vincent. 'Cybersecurity and the Arms Industry'. In *SIPRI Arms Yearbook 2013*, 218–26. Oxford: Oxford University Press, 2013.
Bronk, Christopher, and Eneken Tikk-Ringas. 'The Cyber Attack on Saudi Aramco'. *Survival* 55, no. 2 (1 May 2013): 81–96.
Bueger, Christian. 'From Expert Communities to Epistemic Arrangements: Situating Expertise in International Relations'. In *The Global Politics of Science and Technology - Vol. 1*, edited by Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, 39–54. Global Power Shift. Springer Berlin Heidelberg, 2014.
———. 'Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy'. *International Political Sociology* 9, no. 1 (1 March 2015): 1–18.
Carr, Madeline. 'Internet Freedom, Human Rights and Power'. *Australian Journal of International Affairs* 67, no. 5 (1 November 2013): 621–37.
———. 'Power Plays in Global Internet Governance'. *Millennium* 43, no. 2 (1 January 2015): 640–59.
Chalcraft, John. 'Egypt's 25 January Uprising, Hegemonic Contestation, and the Explosion of the Poor'. In *The New Middle East: Protest And Revolution In The Arab World*, edited by Fawaz A. Gerges, 155–79. New York: Cambridge University Press, 2013.
Cohn, Carol. 'Sex and Death in the Rational World of Defense Intellectuals'. *Signs: Journal of Women in Culture and Society* 12, no. 4 (1 July 1987): 687–718.
Coleman, E. Gabriella, and Alex Golub. 'Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism'. *Anthropological Theory* 8, no. 3 (1 September 2008): 255–77.
Coleman, Gabriella. 'The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld'. *Anthropological Quarterly* 83, no. 1 (4 March 2010): 47–72.
Collective, C.A.S.E. 'Critical Approaches to Security in Europe: A Networked Manifesto'. *Security Dialogue* 37, no. 4 (1 December 2006): 443–87.
Cornish, Paul. 'Governing Cyberspace through Constructive Ambiguity'. *Survival* 57, no. 3 (4 May 2015): 153–76.
Cornut, Jérémie. 'Diplomacy, Agency, and the Logic of Improvisation and Virtuosity in Practice'. *European Journal of International Relations* 24, no. 3 (8 September 2017).
Cox, Robert W. 'Social Forces, States and World Orders: Beyond International Relations Theory'. *Millennium* 10, no. 2 (1 June 1981): 126–55.
Cross, Mai'a K. Davis. 'Rethinking Epistemic Communities Twenty Years Later'. *Review of International Studies* 39, no. 01 (January 2013): 137–160.
Dann, Gary Elijah, and Neil Haddow. 'Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet'. *Journal of Business Ethics* 79, no. 3 (1 May 2008): 219–34.

Deibert, Ronald J. ‘Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace’. *Millennium - Journal of International Studies* 32, no. 3 (1 December 2003): 501–30.
———. ‘Circuits of Power: Security in the Internet Environment’. In *Information Technologies and Global Politics*, edited by James N. Rosenau and J. P. Singh, 115–42. Albany, NY: State University of New York Press, 2002.
———. ‘The Virtual Absence of Malice: Cyber Security and Threat Politics’. *International Studies Review* 11, no. 2 (1 June 2009): 373–75.
Deibert, Ronald J., and Rafal Rohozinski. ‘Risking Security: Policies and Paradoxes of Cyberspace Security’. *International Political Sociology* 4, no. 1 (1 March 2010): 15–32.
Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. ‘Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War’. *Security Dialogue* 43, no. 1 (1 February 2012): 3–24.
Dixon, Jennifer M. ‘Rhetorical Adaptation and Resistance to International Norms’. *Perspectives on Politics* 15, no. 1 (March 2017): 83–99.
Doran, Michael. ‘Egypt: Pan-Arabism in Historical Context’. In *Diplomacy in the Middle East: The International Relations of Regional and Outside Powers*, edited by L. Carl Brown, 97–120. London; New York: I.B.Tauris, 2003.
Douglas, Mary. ‘Risk as a Forensic Resource’. *Daedalus* 119, no. 4 (1990): 1–16.
Drezner, Daniel W. ‘The Global Governance of the Internet: Bringing the State Back In’. *Political Science Quarterly* 119, no. 3 (2004): 477–98.
Duffy, Matt. ‘Arab Media Regulations: Identifying Restraints on Freedom of the Press in the Laws of Six Arabian Peninsula Countries’. *Berkeley Journal of Middle Eastern & Islamic Law* 6, no. 1 (1 April 2014): 1.
Dunn Cavelty, Myriam. ‘Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities’. *Science and Engineering Ethics*, 2014.
Dunn Cavelty, Myriam, and Mark Daniel Jaeger. ‘(In)Visible Ghosts in the Machine and the Powers That Bind: The Relational Securitization of Anonymous’. *International Political Sociology* 9, no. 2 (1 June 2015): 176–94.
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. NATO CCDCOE, 2016.
Fandy, Mamoun. ‘Information Technology, Trust, and Social Change in the Arab World’. *Middle East Journal* 54, no. 3 (2000): 378–94.
Faraj, Samar, and Bijan Azad. ‘The Materiality of Technology: An Affordance Perspective’. In *Materiality and Organizing: Social Interaction in a Technological World*, edited by Paul Leonardi, Bonnie A. Nardi, and Jannis Kallinikos. Oxford: Oxford University Press, 2013.
Fawcett, Louise. ‘Alliances and Regionalism in the Middle East’. In *International Relations of the Middle East*, edited by Louise Fawcett, 197–217. Oxford: Oxford University Press, 2013.
———. ‘Exploring Regional Domains: A Comparative History of Regionalism’. *International Affairs* 80, no. 3 (1 May 2004): 429–46.
Fidler, Mailyn. ‘Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, Summer 2015. https://papers.ssrn.com/abstract=2706199.
Finnemore, Martha. ‘Cultivating International Cyber Norms’. In *America’s Cyber Future: Security and Prosperity in the Information Age*, edited by Kristin M. Lord, Mike McConnell, Peter Schwartz, Richard Fontaine, Travis Sharp, and Will Rogers. Washington, D.C: CNAS, 2011.
Finnemore, Martha, and Duncan B. Hollis. ‘Constructing Norms for Global Cybersecurity’. *American Journal of International Law* 110, no. 3 (July 2016): 425–79.
Finnemore, Martha, and Kathryn Sikkink. ‘International Norm Dynamics and Political Change’. *International Organization* 52, no. 4 (1998): 887–917.
Fischerkeller, Michael P., and Richard J. Harknett. ‘Deterrence Is Not a Credible Strategy for Cyberspace’. *Orbis* 61, no. 3 (1 January 2017): 381–93.
Flyverbom, Mikkel, Ronald Deibert, and Dirk Matten. ‘The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business’. *Business & Society*, 26 August 2017.

Gartzke, Erik, and Jon R. Lindsay. ‘Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace’. *Security Studies* 24, no. 2 (3 April 2015): 316–48.
Gause, F. Gregory III. ‘Oil and Political Mobilization in Saudi Arabia’. In *Saudi Arabia in Transition: Insights on Social, Political, Economic and Religious Change*, edited by Bernard Haykel, Thomas Hegghammer, and Stéphane Lacroix. New York, NY: Cambridge University Press, 2015.
George, Jim. ‘Realist “Ethics”, International Relations, and Post-Modernism: Thinking Beyond the Egoism-Anarchy Thematic’. *Millennium* 24, no. 2 (1 July 1995): 195–223.
Giles, Keir, and William Hagestad II. ‘Divided by a Common Language: Cyber Definitions in Chinese, Russian and English’. In *2013 5th International Conference on Cyber Conflict*, edited by K Podins, J Stinissen, and M Maybaum. Tallinn: NATO CCDCOE, 2013.
Gray, Matthew. ‘A Theory of “Late Rentierism” in the Arab States of the Gulf’. *Center for International and Regional Studies, Georgetown University* Occasional Paper (2011).
Grigsby, Alex. ‘The End of Cyber Norms’. *Survival* 59, no. 6 (2 November 2017): 109–22.
Haas, Peter M. ‘Introduction: Epistemic Communities and International Policy Coordination’. *International Organization* 46, no. 1 (1992): 1–35.
Hagmann, Jonas, and Myriam Dunn Cavelty. ‘National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity’. *Security Dialogue* 43, no. 1 (1 February 2012): 79–96.
Hall, Peter, Claude Heath, and Lizzie Coles-Kemp. ‘Critical Visualization: A Case for Rethinking How We Visualize Risk and Security’. *Journal of Cybersecurity* 1, no. 1 (1 September 2015): 93–108.
Hansen, Lene. ‘How Images Make World Politics: International Icons and the Case of Abu Ghraib’. *Review of International Studies* 41, no. 2 (April 2015): 263–88.
———. ‘The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School’. *Millennium* 29, no. 2 (1 June 2000): 285–306.
———. ‘Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis*’. *European Journal of International Relations* 17, no. 1 (1 March 2011): 51–74.
Hansen, Lene, and Helen Nissenbaum. ‘Digital Disaster, Cyber Security, and the Copenhagen School’. *International Studies Quarterly* 53, no. 4 (1 December 2009): 1155–75.
Harknett, Richard J., and Joseph S. Nye. ‘Is Deterrence Possible in Cyberspace?’ *International Security* 42, no. 2 (1 November 2017): 196–99.
Heck, Axel, and Gabi Schlag. ‘Securitizing Images: The Female Body and the War in Afghanistan’. *European Journal of International Relations* 19, no. 4 (1 December 2013): 891–913.
Hertog, Steffen. ‘Defying the Resource Curse: Explaining Successful State-Owned Enterprises in Rentier States’. *World Politics* 62, no. 2 (April 2010): 261–301.
———. ‘The Private Sector and Reform in the Gulf Cooperation Council’. Kuwait Programme on Development, Governance and Globalisation in the Gulf States, July 2013.
Holmwood, John. ‘The Challenge of Global Social Inquiry’. *Sociological Research Online* 14(4)13 (31 August 2009).
Hönke, Jana, and Markus-Michael Müller. ‘Governing (in)Security in a Postcolonial World: Transnational Entanglements and the Worldliness of “Local” Practice’. *Security Dialogue* 43, no. 5 (1 October 2012): 383–401.
Hopf, Ted. ‘The Logic of Habit in International Relations’. *European Journal of International Relations* 16, no. 4 (1 December 2010): 539–61.
Howard, Philip N. ‘Network Ethnography and the Hypermedia Organization: New Media, New Organizations, New Methods’. *New Media & Society* 4, no. 4 (1 December 2002): 550–74.
Howard, Philip N., and Muzzamil M. Hussain. ‘The Role of Digital Media’. In *Democratization and Authoritarianism in the Arab World*, edited by Larry Diamond and Marc F. Plattner, 186–202. Baltimore: Johns Hopkins University Press, 2014.
Hurel, Louise Marie, and Luisa Cruz Lobato. ‘Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs’. *Journal of Cyber Policy* 3, no. 1 (27 April 2018): 1–16.
Hurwitz, Roger. ‘The Play of States: Norms and Security in Cyberspace’. *American Foreign Policy Interests* 36, no. 5 (3 September 2014): 322–31.
Huysmans, Jef. ‘Security! What Do You Mean?: From Concept to Thick Signifier’. *European Journal of International Relations* 4, no. 2 (1 June 1998): 226–55.
Jarvis, Lee, Stuart Macdonald, and Lella Nouri. ‘The Cyberterrorism Threat: Findings from a Survey of Researchers’. *Studies in Conflict & Terrorism* 37, no. 1 (2 January 2014): 68–90.

Kello, Lucas. ‘Private-Sector Cyberweapons: Strategic and Other Consequences’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 15 June 2016. https://papers.ssrn.com/abstract=2836196.
———. ‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft’. *International Security* 38, no. 2 (1 October 2013): 7–40.
Khiabany, Gholam. ‘Technologies of Liberation and/or Otherwise’. *International Journal of Middle East Studies* 47, no. 2 (May 2015): 348–53.
Krook, Mona Lena, and Jacqui True. ‘Rethinking the Life Cycles of International Norms: The United Nations and the Global Promotion of Gender Equality’. *European Journal of International Relations* 18, no. 1 (1 March 2012): 103–27.
Kubik, Jan. ‘Ethnography of Politics’. In *Political Ethnography: What Immersion Contributes to the Study of Power*, edited by Edward Schatz. Chicago: University of Chicago Press, 2009.
Kutz, Christopher. ‘How Norms Die: Torture and Assassination in American Security Policy’. *Ethics & International Affairs* 28, no. 4 (2014): 425–49.
Leander, Anna. ‘The Power to Construct International Security: On the Significance of Private Military Companies’. *Millennium* 33, no. 3 (1 June 2005): 803–25.
———. ‘Thinking Tools’. In *Qualitative Methods in International Relations: A Pluralist Guide*, edited by A. Klotz and D. Prakash. Basingstoke England; New York: Palgrave Macmillan, 2008.
Lee, Robert M., and Thomas Rid. ‘OMG Cyber!’ *The RUSI Journal* 159, no. 5 (3 September 2014): 4–12.
Leech, Beth L. ‘Asking Questions: Techniques for Semistructured Interviews’. *Political Science & Politics* 35, no. 4 (December 2002): 665–68.
Liverman, Diana M. ‘Conventions of Climate Change: Constructions of Danger and the Dispossession of the Atmosphere’. *Journal of Historical Geography* 35, no. 2 (1 April 2009): 279–96.
Manjikian, Mary McEvoy. ‘From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik’. *International Studies Quarterly* 54, no. 2 (2010): 381–401.
March, James G., and Johan P. Olsen. ‘The Institutional Dynamics of International Political Orders’. *International Organization* 52, no. 4 (1998): 943–69.
Matthews, Ron. ‘The UK Offset Model: From Participation to Engagement’. *RUSI*, 29 July 2014.
McCourt, David. ‘Practice Theory and Relationism as the New Constructivism’. *International Studies Quarterly* 60, no. 3 (2016): 475–85.
Milliken, Jennifer. ‘The Study of Discourse in International Relations: A Critique of Research and Methods’. *European Journal of International Relations* 5, no. 2 (1 June 1999): 225–54.
Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. ‘Internet Security and Networked Governance in International Relations’. *International Studies Review* 15, no. 1 (1 March 2013): 86–104.
Murphy, Emma C. ‘Agency and Space: The Political Impact of Information Technologies in the Gulf Arab States’. *Third World Quarterly* 27, no. 6 (2006): 1059–83.
———. ‘Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere’. *International Studies Quarterly* 53, no. 4 (1 December 2009): 1131–53.
Nabi, Syed Irfan, Abdulrahman A. Mirza, and Khaled Alghathbar. ‘Information Assurance in Saudi Organizations – An Empirical Study’. In *Security Technology, Disaster Recovery and Business Continuity*, 18–28. Springer, Berlin, Heidelberg, 2010.
Naim, Abd Allah Ahmad. ‘The Interdependence of Religion, Secularism, and Human Rights: Prospects for Islamic Societies’. *Common Knowledge* 11, no. 1 (11 January 2005): 56–80.
Nexon, Daniel H., and Vincent Pouliot. ‘“Things of Networks”: Situating ANT in International Relations’. *International Political Sociology* 7, no. 3 (1 September 2013): 342–45.
Nissenbaum, Helen. ‘Hackers and the Contested Ontology of Cyberspace’. *New Media & Society* 6, no. 2 (1 April 2004): 195–217.
Nurse, J. R. C., O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty. ‘Understanding Insider Threat: A Framework for Characterising Attacks’. In *2014 IEEE Security and Privacy Workshops*, 214–28, 2014.
Nye, Joseph S. ‘Deterrence and Dissuasion in Cyberspace’. *International Security* 41, no. 3 (1 January 2017): 44–71.
———. ‘Nuclear Lessons for Cyber Security?’ *Strategic Studies Quarterly* 5, no. 4 (2011): 18.
Paris, Roland. ‘Human Security: Paradigm Shift or Hot Air?’ *International Security* 26, no. 2 (1 October 2001): 87–102.

Paul, James, and Joe Stork. ‘The Middle East and Human Rights’. *Middle East Research and Information Project* Winter, no. 149 (1987). https://perma.cc/6D7S-ELJ8.
Petersen, Karen Lund. ‘Risk Analysis – A Field within Security Studies?’ *European Journal of International Relations* 18, no. 4 (1 December 2012): 693–717.
Pouliot, Vincent. ‘The Logic of Practicality: A Theory of Practice of Security Communities’. *International Organization* 62, no. 2 (April 2008): 257–88.
Price, Richard. ‘A Genealogy of the Chemical Weapons Taboo’. *International Organization* 49, no. 1 (1995): 73–103.
Quigley, Kevin, Calvin Burns, and Kristen Stallard. ‘“Cyber Gurus”: A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection’. *Government Information Quarterly* 32, no. 2 (April 2015): 108–17.
Raymond, Mark. ‘Puncturing the Myth of the Internet as a Commons’. *Georgetown Journal of International Affairs*, no. Special Issue (2013): 5–15.
Raymond, Mark, and Laura DeNardis. ‘Multistakeholderism: Anatomy of an Inchoate Global Institution’. *International Theory* 7, no. 3 (November 2015): 572–616.
Rid, Thomas. ‘Cyber War Will Not Take Place’. *Journal of Strategic Studies* 35, no. 1 (1 February 2012): 5–32.
Rishmawi, Mervat. ‘The Arab Charter on Human Rights and the League of Arab States: An Update’. *Human Rights Law Review* 10, no. 1 (1 March 2010): 169–78.
Risse, Thomas. ‘“Let’s Argue!”: Communicative Action in World Politics’. *International Organization* 54, no. 1 (2000): 1–39.
Rogan, Eugene. ‘Rise and Fall’. *Index on Censorship* 25, no. 2 (1 March 1996): 43–49.
Rubinstein, Ira, and Michael Hintze. ‘Export Controls on Encryption Software’. In *Coping With US Export Controls 2000*. Practising Laws Institute, 2000.
Seabrooke, Leonard. ‘Epistemic Arbitrage: Transnational Professional Knowledge in Action’. *Journal of Professions and Organization* 1, no. 1 (1 March 2014): 49–64.
Shires, James, and Max Smeets. ‘Contesting “Cyber”’. New America Foundation, December 2017. https://perma.cc/RJ5B-GQXT.
———. ‘What Do We Talk About When We Talk About “Cyber”?’ *Working Paper*. Accessed 8 February 2017. https://papers.ssrn.com/abstract=2860839.
Simon, Stephanie, and Marieke de Goede. ‘Cybersecurity, Bureaucratic Vitalism and European Emergency’. *Theory, Culture & Society* 32, no. 2 (1 March 2015): 79–106.
Slack, Chelsey. ‘Wired yet Disconnected: The Governance of International Cyber Relations’. *Global Policy* 7, no. 1 (1 February 2016): 69–78.
Slayton, Rebecca. ‘What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment’. *International Security* 41, no. 3 (1 January 2017): 72–109.
Smeets, Max. ‘A Matter of Time: On the Transitory Nature of Cyberweapons’. *Journal of Strategic Studies* 42, no. 1–2 (16 February 2017): 1–28.
Stay, Ronald. ‘Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann’. *Georgia State University Law Review* 13, no. 2 (1996).
Stevens, Tim. ‘A Cyberwar of Ideas? Deterrence and Norms in Cyberspace’. *Contemporary Security Policy* 33, no. 1 (1 April 2012): 148–70.
———. ‘Cyberweapons: An Emerging Global Governance Architecture’. *Palgrave Communications* 3, no. 16102 (10 January 2017).
———. ‘Cyberweapons: Power and the Governance of the Invisible’. *International Politics* 55, no. 3 (1 May 2018): 482–502.
Stone, John. ‘Cyber War Will Take Place!’ *Journal of Strategic Studies* 36, no. 1 (1 February 2013): 101–8.
Sundaramurthy, S. C., J. McHugh, X. S. Ou, S. R. Rajagopalan, and M. Wesch. ‘An Anthropological Approach to Studying CSIRTs’. *IEEE Security Privacy* 12, no. 5 (September 2014): 52–60.
Sundaramurthy, Sathya Chandran, Jacob Case, Tony Truong, Loai Zomlot, and Marcel Hoffmann. ‘A Tale of Three Security Operation Centers’. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, 43–50. SIW ’14. New York, NY, USA: ACM, 2014.
Tanczer, Leonie Maria. ‘Hacktivism and the Male-Only Stereotype’. *New Media & Society*, 14 January 2015.

Tikk-Ringas, Eneken. ‘International Cyber Norms Dialogue as an Exercise of Normative Power’. *Georgetown Journal of International Affairs* 17, no. 3 (2017): 47–59.
Ulrichsen, Kristian Coates. ‘Internal and External Security in the Arab Gulf States’. *Middle East Policy* 16, no. 2 (1 June 2009): 39–58.
Vogel, Rebecca. ‘Closing the Cybersecurity Skills Gap’. *Salus Journal* 4, no. 2 (2016): 32–46.
Vuori, Juha A. ‘A Timely Prophet? The Doomsday Clock as a Visualization of Securitization Moves with a Global Referent Object’. *Security Dialogue* 41, no. 3 (1 June 2010): 255–77.
Waelbers, Katinka, and Philipp Dorstewitz. ‘Ethics in Actor Networks, or: What Latour Could Learn from Darwin and Dewey’. *Science and Engineering Ethics* 20, no. 1 (March 2014): 23–40.
Wæver, Ole. ‘Politics, Security, Theory’. *Security Dialogue* 42, no. 4–5 (1 August 2011): 465–80.
Watson, Scott D. ‘“Framing” the Copenhagen School: Integrating the Literature on Threat Construction’. *Millennium* 40, no. 2 (1 January 2012): 279–301.
Webb, Edward. ‘Holding Back The Flood: Regimes of Censorship in the Middle East & North Africa in Comparative Perspective’. *German Media Journal*, no. 2012/01 (May 2012).
Wedeen, Lisa. ‘Reflections on Ethnographic Work in Political Science’. *Annual Review of Political Science* 13, no. 1 (1 May 2010): 255–72.
Welsh, Jennifer M. ‘Norm Contestation and the Responsibility to Protect’. *Global Responsibility to Protect* 5, no. 4 (1 January 2013): 365–96.
Wheeler, Deborah L. ‘Egypt: Building an Information Society for International Development’. *Review of African Political Economy* 30, no. 98 (1 December 2003): 627–42.
Wildavsky, Aaron. ‘The Open-Ended, Semistructured Interview: An (Almost) Operational Guide’. In *Craftways: On the Organization of Scholarly Work*, by Aaron Wildavsky. New Brunswick, N.J: Transaction Publishers, 1993.
Williams, Michael C. ‘Words, Images, Enemies: Securitization and International Politics’. *International Studies Quarterly* 47, no. 4 (1 December 2003): 511–31.
Wolfers, Arnold. ‘“National Security” as an Ambiguous Symbol’. *Political Science Quarterly* 67, no. 4 (1952): 481–502.
Zajko, Mike. ‘Canada’s Cyber Security and the Changing Threat Landscape’. *Critical Studies on Security* 3, no. 2 (4 May 2015): 147–61.
Zayani, Mohamed. ‘Transnational Media, Regional Politics and State Security: Saudi Arabia between Tradition and Modernity’. *British Journal of Middle Eastern Studies* 39, no. 3 (1 December 2012): 307–27.
Zwingel, Susanne. ‘How Do Norms Travel? Theorizing International Women’s Rights in Transnational Perspective1’. *International Studies Quarterly* 56, no. 1 (1 March 2012): 115–29.

Books

Abdulla, Rasha A. *The Internet in the Arab World: Egypt and Beyond*. New York: Peter Lang Publishing, 2007.
Abrahamsen, Rita, and Anna Leander, eds. *Routledge Handbook of Private Security Studies*. London; New York: Routledge, 2015.
Abrahamsen, Rita, and Michael C. Williams. *Security Beyond the State: Private Security in International Politics*. Cambridge; New York: Cambridge University Press, 2010.
Abu-Lughod, Lila, ed. *Remaking Women: Feminism and Modernity in the Middle East*. Princeton, N.J: Princeton University Press, 1998.
Acuto, M., and S. Curtis. *Reassembling International Theory: Assemblage Thinking and International Relations*. Springer, 2013.
Adler, Emanuel, and Vincent Pouliot, eds. *International Practices*. Cambridge; New York: Cambridge University Press, 2011.
Adler, Emmanuel, and Michael N. Barnett, eds. *Security Communities*. Cambridge; New York: Cambridge University Press, 2008.
Adler-Nissen, Rebecca, ed. *Bourdieu in International Relations: Rethinking Key Concepts in IR*. New York: Routledge, 2013.

Aldrich, Richard. *GCHQ*. London: HarperPress, 2010.
Alexander, James. 'Promoting Security Imaginaries: An Analysis of the Market for Everyday Security Solutions'. PhD Thesis, University of Manchester, 2014.
Almezaini, Khalid, and Jean-Marc Rickli, eds. *The Small Gulf States*. London; New York: Routledge, 2016.
Al-Rasheed, Madawi. *A History of Saudi Arabia*. New York: Cambridge University Press, 2010.
———. *A Most Masculine State: Gender, Politics and Religion in Saudi Arabia*. Cambridge: Cambridge University Press, 2013.
Alston, Philip, ed. *Non-State Actors and Human Rights*. Oxford; New York: Oxford University Press, 2005.
Amoore, Louise. *The Politics of Possibility: Risk and Security Beyond Probability*. Durham: Duke University Press, 2013.
Amoureux, Jack L., and Brent J. Steele, eds. *Reflexivity and International Relations: Positionality, Critique, and Practice*. London; New York: Routledge, 2015.
Aradau, Claudia, Jef Huysmans, Andrew Neal, and Nadine Voelkner, eds. *Critical Security Methods: New Frameworks for Analysis*. London; New York: Routledge, 2014.
Ayubi, Nazih. *Political Islam: Religion and Politics in the Arab World*. London: Routledge, 1993.
Balzacq, Thierry, ed. *Securitization Theory*. Oxford; New York: Routledge, 2010.
Barnett, Michael N. *Dialogues in Arab Politics: Negotiations in Regional Order*. New York: Columbia University Press, 1998.
Bauman, Zygmunt. *Liquid Modernity*. Cambridge, UK: Malden, MA: Polity Press, 2000.
Beblawi, Hazem, and Giacomo Luciani, eds. *The Rentier State*. Routledge, 2016.
Beck, Ulrich. *Risk Society: Towards a New Modernity*. London: SAGE, 1992.
Beitz, Charles R. *The Idea of Human Rights*. Oxford: Oxford University Press, USA, 2011.
Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Adelphi Series. Routledge, 2011.
Bob, Clifford. *The Global Right Wing and the Clash of World Politics*. New York: Cambridge University Press, 2012.
Bonine, Michael E., Abbas Amanat, and Michael Ezekiel Gasper, eds. *Is There a Middle East?: The Evolution of a Geopolitical Concept*. Stanford, California: Stanford University Press, 2011.
Booth, Ken, ed. *Critical Security Studies and World Politics*. Boulder, Colo: Lynne Rienner Publishers, 2004.
Bourdieu, Pierre. *The Logic of Practice*. Cambridge: Polity Press, 1992.
Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. London: Hurst, 2017.
Burchell, Graham, Colin Gordon, and Peter Miller, eds. *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press, 1991.
Buzan, Barry, and Eric Herring. *The Arms Dynamic in World Politics*. Boulder: Lynne Rienner Publishers, 1998.
Buzan, Barry, and Ole Waever. *Regions and Powers: The Structure of International Security*. Cambridge; New York: Cambridge University Press, 2003.
Buzan, Barry, Ole Waever, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, Colo: Lynne Rienner Publishers, 1997.
Chase, Anthony, and Amr Hamzawy, eds. *Human Rights in the Arab World: Independent Voices*. Philadelphia: University of Pennsylvania Press, 2008.
Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press, 2012.
Cook, Steven A. *The Struggle for Egypt: From Nasser to Tahrir Square*. Oxford: Oxford University Press, 2013.
Dalacoura, Katerina. *Islam, Liberalism and Human Rights*. London; New York: I.B.Tauris, 2003.
Davidson, Christopher M. *Dubai: The Vulnerability of Success*. London: Hurst, 2009.
———. *The United Arab Emirates: A Study in Survival*. Lynne Rienner Publishers, 2005.
Deibert, Ron J. *Black Code: Inside the Battle for Cyberspace*. Plattsburgh, NY: Signal Books, 2013.
Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press, 2011.
Deibert, Ronald, Rafal Rohozinski, John Palfrey, and Jonathan Zittrain, eds. *Access Denied: The Practice*

and Policy of Global Internet Filtering. Cambridge, MA: MIT Press, 2008.
DeLanda, Manuel. *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London; New York: Continnuum-3PL, 2006.
Determann, Jorg Matthias. *Historiography in Saudi Arabia: Globalization and the State in the Middle East*. London; New York: I.B.Tauris, 2013.
Dill, Janina. *Legitimate Targets?: Social Construction, International Law And Us Bombing*. Cambridge, UK: Cambridge University Press, 2014.
Dillon, Michael, and Julian Reid. *The Liberal Way of War*. London; New York: Routledge, 2009.
Donnelly, Jack. *Universal Human Rights in Theory and Practice*. Ithaca: Cornell University Press, 2002.
Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics*. London, New York: Routledge, 2008.
Edwards, Rosalind, and Janet Holland. *What Is Qualitative Interviewing?* London: Bloomsbury, 2013.
Erickson, Jennifer. *Dangerous Trade: Arms Exports, Human Rights, and International Reputation*. New York: Columbia University Press, 2015.
Eriksson, Johan, and Giampiero Giacomello. *International Relations and Security in the Digital Age*. Routledge, 2007.
Esposito, John L., Tamara Sonn, and John O. Voll. *Islam and Democracy after the Arab Spring*. Oxford: Oxford University Press, 2016.
Falzon, Mark-Anthony, ed. *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research*. London: Routledge, 2009.
Farrell, Mary, Björn Hettne, and Luk Van Langenhove, eds. *Global Politics of Regionalism: Theory and Practice*. London; Ann Arbor: Pluto Press, 2005.
Fawcett, Louise, and Andrew Hurrell, eds. *Regionalism in World Politics: Regional Organizational and International Order*. New York: Clarendon Press, 1996.
Fierke, Karin M. *Critical Approaches to International Security*. Cambridge: Polity Press, 2007.
Flyvbjerg, Bent. *Making Social Science Matter: Why Social Inquiry Fails and How It Can Succeed Again*. Cambridge: Cambridge University Press, 2011.
Foley, Sean. *The Arab Gulf States: Beyond Oil and Islam*. Boulder, Colo: Lynne Rienner Publishers, 2010.
Frost, Mervyn. *Ethics in International Relations: A Constitutive Theory*. Cambridge; New York: Cambridge University Press, 2008.
Geertz, Clifford. *The Interpretation Of Cultures*. New York: Basic Books, 1977.
Gilby, Nicholas. *Deception in High Places: A History of Bribery in Britain's Arms Trade*. London: Pluto Press, 2014.
Glendon, Mary Ann. *A World Made New*. New York: Random House USA Inc, 2002.
Glynos, Jason, and David Howarth. *Logics of Critical Explanation in Social and Political Theory*. London; New York: Routledge, 2007.
Goldblatt, David, Jonathan Perraton, David Held, and Anthony McGrew. *Global Transformations: Politics, Economics, Culture*. Cambridge, UK: Polity Press, 1999.
Hacking, Ian. *The Social Construction of What?* Cambridge, MA: Harvard University Press, 2000.
Hafner-Burton, Emilie M. *Making Human Rights a Reality*. Princeton, New Jersey: Princeton University Press, 2013.
Hall, Todd H. *Emotional Diplomacy: Official Emotion on the International Stage*. Ithaca; London: Cornell University Press, 2015.
Hansen, Lene. *Security as Practice: Discourse Analysis and the Bosnian War*. New York: Routledge, 2006.
Held, David, and Kristian Ulrichsen, eds. *The Transformation of the Gulf: Politics, Economics and the Global Order*. Oxford; New York: Routledge, 2011.
Henry, Clement Moore, and Robert Springborg. *Globalization and the Politics of Development in the Middle East*. New York: Cambridge University Press, 2010.
Hertog, Steffen. *Princes, Brokers, and Bureaucrats: Oil and the State in Saudi Arabia*. Ithaca: Cornell University Press, 2011.
Hertog, Steffen, Giacomo Luciani, and Marc Valeri, eds. *Business Politics in the Middle East*. London: Hurst, 2013.
Hindess, Barry. *Discourses of Power: From Hobbes to Foucault*. Oxford, UK; Cambridge, Mass., USA: John Wiley & Sons, 1996.
Hirst, Paul, Grahame Thompson, and Simon Bromley. *Globalization in Question*. Cambridge: Polity Press,

2009.
Hosseinioun, Mishana. *The Human Rights Turn and the Paradox of Progress in the Middle East*. New York: Palgrave Macmillan, 2017.
Howard, Philip N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford; New York: Oxford University Press, 2010.
Hurrell, Andrew. *On Global Order: Power, Values, and the Constitution of International Society*. Oxford; New York: Oxford University Press, 2008.
Jackson, Patrick Thaddeus. *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics*. London; New York: Routledge, 2010.
Jones, Richard Wyn. *Security, Strategy and Critical Theory*. Boulder, Colo: Lynne Rienner Publishers, 1999.
Joyce, Miriam. *Bahrain from the Twentieth Century to the Arab Spring*. New York: Palgrave Macmillan, 2012.
Kalathil, Shanthi, and Taylor C. Boas. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, D.C: Brookings Institution Press, 2002.
Kandil, Hazem. *The Power Triangle: Military, Security, and Politics in Regime Change*. Oxford: Oxford University Press, 2016.
Kandiyoti, Deniz, ed. *Gendering the Middle East: Alternative Perspectives*. London: I.B.Tauris, 1995.
Katzenstein, Peter, ed. *The Culture of National Security: Norms and Identity in World Politics*. New York, NY: Columbia University Press, 1996.
Keck, Margaret E., and Kathryn Sikkink. *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press, 1998.
Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.
Kennedy, David. *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy*. Princeton University Press, 2016.
Klotz, A., and D. Prakash, eds. *Qualitative Methods in International Relations: A Pluralist Guide*. Basingstoke England; New York: Palgrave Macmillan, 2008.
Klotz, Audie. *Norms in International Relations: Struggle Against Apartheid*. Ithaca: Cornell University Press, 2000.
Koskenniemi, Martti. *From Apology to Utopia: The Structure of International Legal Argument*. New York: Cambridge University Press, 2006.
Kratochwil, Friedrich V. *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge: Cambridge University Press, 1991.
Krause, Keith, and Michael C. Williams, eds. *Critical Security Studies: Concepts And Strategies*. London: Routledge, 1997.
Kuckartz, Udo. *Qualitative Text Analysis*. Los Angeles: SAGE, 2014.
Latour, Bruno. *On the Modern Cult of the Factish Gods*. Durham NC; London: Duke University Press Books, 2010.
———. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford; New York: Oxford University Press, 2007.
Lauren, Paul Gordon. *The Evolution of International Human Rights: Visions Seen*. Philadelphia: University of Pennsylvania Press, 2011.
Lawson, Fred Haley. *Bahrain: The Modernization of Autocracy*. Westview Press, 1989.
Legrenzi, Matteo. *Beyond Regionalism?: Regional Cooperation, Regionalism and Regionalization in the Middle East*. Edited by Cilja Harders. Oxford: Routledge, 2008.
———. *The GCC and the International Relations of the Gulf: Diplomacy, Security and Economic Coordination in a Changing Middle East*. I.B.Tauris, 2015.
Lessig, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.
Levy, Steven. *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*. Penguin, 2001.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2010.
———. *Crisis and Escalation in Cyberspace*. Santa Monica: RAND Corporation, 2012.
———. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Lockman, Zachary. *Contending Visions of the Middle East: The History and Politics of Orientalism*. Cambridge, UK; New York: Cambridge University Press, 2009.
Luke, Timothy W. *Ecocritique: Contesting the Politics of Nature, Economy, and Culture*. Minneapolis: University of Minnesota Press, 1997.
Lynch, Marc. *The Arab Uprising: The Unfinished Revolutions of the New Middle East*. New York: PublicAffairs, 2013.
———. *Voices of the New Arab Public: Iraq, Al-Jazeera, and Middle East Politics Today*. New York, NY: Columbia University Press, 2007.
Matthiesen, Toby. *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring That Wasn't*. Stanford, California: Stanford University Press, 2013.
———. *The Other Saudis: Shiism, Dissent And Sectarianism*. New York, NY: Cambridge University Press, 2014.
Mayer, Ann. *Islam and Human Rights: Tradition and Politics*. Boulder, Colo: Westview Press, 2012.
Mitchell, Timothy. *Carbon Democracy: Political Power in the Age of Oil*. London: Verso Books, 2013.
———. *Colonising Egypt*. Berkeley: University of California Press, 1992.
———. *Rule of Experts: Egypt, Techno-Politics, Modernity*. Berkeley: University of California Press, 2002.
Monshipouri, Mahmood. *Muslims in Global Politics: Identities, Interests, and Human Rights*. Philadelphia: University of Pennsylvania Press, 2012.
Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs, 2012.
Newell, Peter. *Climate Capitalism: Global Warming And The Transformation Of The Global Economy*. London: Cambridge University Press, 2010.
Niblock, Tim. *Saudi Arabia: Power, Legitimacy and Survival*. London: Routledge, 2006.
Niblock, Tim, and Monica Malik. *The Political Economy of Saudi Arabia*. Oxford; New York: Routledge, 2007.
Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
Ong, Aihwa, and Stephen J Collier, eds. *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*. Malden, MA: Wiley-Blackwell, 2004.
Owtram, Francis. *A Modern History of Oman: Formation of the State since 1920*. London; New York: I.B.Tauris, 2004.
Parpart, Jane L., and Marysia Zalewski, eds. *Rethinking the Man Question: Sex, Gender and Violence in International Relations: 1*. London: New York: Zed Books, 2008.
Perkovich, George. *Understanding Cyber Conflict: Fourteen Analogies*. Edited by Vice President for Studies George Perkovich. Washington, DC: Georgetown University Press, 2018.
Potter, Laurence, ed. *The Persian Gulf in Modern Times: People, Ports, and History*. New York: Palgrave Macmillan, 2014.
Power, Michael. *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos, 2004.
Powers, Shawn M., and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press, 2015.
Price, Richard M., ed. *Moral Limit and Possibility in World Politics*. Cambridge; New York: Cambridge University Press, 2008.
Richards, Alan, John Waterbury, Melanie Cammett, and Ishac Diwan. *A Political Economy of the Middle East: Third Edition*. Boulder: Westview Press, 2013.
Rid, Thomas. *Rise of the Machines: The Lost History of Cybernetics*. Scribe UK, 2017.
Risse, Thomas, Stephen C. Ropp, and Kathryn Sikkink. *The Persistent Power of Human Rights: From Commitment to Compliance*. Cambridge: Cambridge University Press, 2013.
Risse-Kappen, Thomas, Stephen C. Ropp, and Kathryn Sikkink. *The Power of Human Rights: International Norms and Domestic Change*. Cambridge University Press, 1999.
Rogan, Eugene. *The Arabs: A History*. Penguin, 2012.
Rose, Nikolas. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press, 2012.
Rugh, Andrea B. *The Political Culture of Leadership in the United Arab Emirates*. Basingstoke: Palgrave Macmillan, 2010.
Rugh, William A. *The Arab Press: News Media and Political Process in the Arab World*. Syracuse, N.Y:

Syracuse University Press, 1987.
Sakr, Naomi. *Satellite Realms: Transnational Television, Globalization and the Middle East*. London: I.B.Tauris, 2002.
Saleh, Nivien. *Third World Citizens and the Information Technology Revolution*. London; New York: Palgrave MacMillan, 2010.
Sandholtz, Wayne, and Kendall Stiles. *International Norms and Cycles of Change*. Oxford; New York: Oxford University Press, 2008.
Sanger, David E. *Confront and Conceal*. New York: Penguin Random House, 2013.
Schatz, Edward, ed. *Political Ethnography: What Immersion Contributes to the Study of Power*. Chicago: University of Chicago Press, 2009.
Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge England ; New York: NATO CCDCOE, Cambridge University Press, 2013.
Seabrooke, Leonard, and Brett Bowden, eds. *Global Standards of Market Civilization*. London: Routledge, 2007.
Shepherd, Laura J., ed. *Critical Approaches to Security*. London; New York: Routledge, 2012.
Simmons, Beth A. *Mobilizing for Human Rights: International Law in Domestic Politics*. Cambridge; New York: Cambridge University Press, 2011.
Springborg, Robert. *Egypt*. Cambridge, UK: Polity Press, 2017.
Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press, 2015.
Tannenwald, Nina. *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945*. Cambridge: Cambridge University Press, 2007.
Thomas, Daniel C. *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism*. Princeton, N.J: Princeton University Press, 2001.
Valeri, Mark. *Oman: Politics and Society in the Qaboos State*. C Hurst & Co Publishers Ltd, 2017.
Valeriano, Brandon, and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, 2015.
Vatikiotis, P. J. *The History of Modern Egypt: From Muhammad Ali to Mubarak*. London: Weidenfeld & Nicolson, 1991.
Vitalis, Robert. *America's Kingdom: Mythmaking on the Saudi Oil Frontier*. London: Verso Books, 2009.
Waltz, Susan E. *Human Rights and Reform: Changing the Face of North African Politics*. Berkeley: University of California Press, 1995.
Wheeler, Deborah L. *The Internet In The Middle East: Global Expectations And Local Imaginations In Kuwait*. Albany: State University of New York Press, 2005.
Whidden, James. *Monarchy and Modernity in Egypt: Politics, Islam and Neo-Colonialism Between the Wars*. London; New York: I.B.Tauris, 2013.
Wiener, Antje. *A Theory of Contestation*. New York: Springer, 2014.
Wilford, Hugh. *America's Great Game*. New York: Basic Books, 2014.
Yanai, Shaul. *Political Transformation of Gulf Tribal States: Elitism & the Social Contract in Kuwait, Bahrain & Dubai, 1918-1970s*. Brighton: Sussex Academic Press, 2014.
Yanow, Dvora, and Peregrine Schwartz-Shea. *Interpretation and Method: Empirical Research Methods and the Interpretive Turn*. London; New York: Routledge, 2013.
Yergin, Daniel. *The Prize: The Epic Quest for Oil, Money & Power*. London; New York: Simon & Schuster, 2009.
Zahlan, Rosemary Said. *The Making of the Modern Gulf States: Kuwait, Bahrain, Qatar, the United Arab Emirates and Oman*. Ithaca: Ithaca Press, 1998.
Zetter, Kim. *Countdown to Zero Day*. New York: Penguin Random House, 2014.
Zimmermann, Lisbeth. *Global Norms with a Local Face: Rule-of-Law Promotion and Norm Translation*. Cambridge, UK; New York: Cambridge University Press, 2017.

Arabic sources

Al-Barqawi, ʿAbdallah. 'Mutalabat Bimuʿaqaba Murawaji Shaʾiʿat "Al-Qurarat" ʿabr Muwaqiʿa Al-Tawassul [Demands to Punish the Promotion of "Low" Rumours on Social Media]'. Sabq, 18

November 2017. https://perma.cc/5K8R-SV5G.
———. ‘Tanfiz Hukm Al-Jild ʿala Raʾif Badawi Bisubbub ʿibarat Kufriyya Wa ʿuquq Walidihi [Sentence of Lashes Imposed against Raif Badawi for Expressions of Unbelief and Insulting His Father]’. Sabq, 9 January 2015. https://perma.cc/Q99Y-5F39.
———. ‘ʿajil… “Suqur Al-Qatar” Takhtariqu “Hisab Al-Muwatin” [Breaking… “Qatari Falcons” Hack “the Citizen’s Account”]’. Sabq, 2 January 2018. https://perma.cc/U98N-ALN4.
Al-Ghamdi, Muhammad. ‘Muhawalat Ikhtiraq ʾaramku Tahdufu Lil-ʾidrar Bil-Iqtisad Al-Watani Wa Manaʿa Tadaffuq Al-Zait ʾila Al-ʾaswaq Al-Mahaliyya Wa Al-ʿalamiyya [The Attempted Attack of Aramco Aims to Damage the National Economy and Stop the Flow of Oil to Local and Global Markets]’. Al-Riyadh, 10 December 2012. https://perma.cc/55U5-RCFM.
Al-Hawawi, Saʿud. ‘Musadir Khasa: Shabakat Sharikat ʾaramku Tataʿarrad Liʾikhtiraq Wa Almutasabbib Ahad Al-Muwazzifin [Private Sources: Aramco Company Networks Face a Hack and the Cause Is One of Their Employees]’. ʿAlam Al-Tiqniyya, 15 August 2012. https://perma.cc/FHW6-JPUW.
Al-Jalad, Majdi. ‘Infirad: Al-Dakhiliyya Tafridu “Qabda ʾiliktruniyya” ʿala Jaraʾim Shabakat Al-Tawassul Al-Ijtimaʿi [Exclusive: The Ministry of the Interior Imposes “Electronic Grip” on Social Media Crimes]’. Al-Watan, 1 June 2014. https://perma.cc/TCE3-N26A.
Al-Jamiʿat Al-Dawl Al-ʿArabiyya [The Arab League]. ‘Al-Itifaqiyya Al-ʿarabiyya Limukafahat Jaraʾim Tiqniyyat Almuʿalumat [the Arab Convention on Combatting Information Technology Crimes]’. Al-Jamiʿat Al-Dawl Al-ʿArabiyya [The Arab League], 21 December 2010.
Al-Khalifi, ʿAbdallah. ‘Al-Saʿudiyya Tadrusu ʾinshaʾ Hayaʾat Wataniyya Liʾamn Al-Muʿalumat [Saudi Arabia Studies the Formation of a National Centre for Information Security]’. Al-ʿArabiyya, 18 June 2013. https://perma.cc/9CEG-XHP9.
Al-Marjan, ʿAbd Al-Razzaq. ‘ʾiran Taqudu Shaghaban Raqmian Litashjiʿ Al-ʿunf [Iran Leads Digital Subversion to Encourage Violence]’. Okaz, 5 January 2016. https://perma.cc/KAN4-LHW7.
Al-Maʿrawi, ʾAnas. ‘Aramku Taʿtarifu Bitaʿarrud ʾanzimatiha Liʾikhtiraq Kabir [Aramco Admits Its Networks Faced a Large Hack]’. *Aitnews*, 28 August 2012. https://perma.cc/ZC63-Z76W.
Al-Rashid, ʿAbd Al-Rahman. ‘Al-Hujum ʿala Aramku Wa Sad Niu Yurk [The Attacks on Aramco and a New York Dam]’. Al-Sharq Al-ʾAwsat, 27 March 2016. https://perma.cc/K939-HEB9.
Al-Tahir, Muhammad. ‘Taʿliq ʿala Al-Itifaqiyya Al-ʿarabiyya Limukafahat Jaraʾim Tiqniyyat Almuʿalumat [Comments on the Arab Convention for Combatting Information Technology Crimes]’. Muʾassasat Huriyyat Al-Fikr Wa Al-Taʿbir [Foundation for the freedom of thought and expression], 12 March 2015. https://perma.cc/DUB8-6END.
Al-ʿAli, Nasir. ‘Markaz Watani Lil-ʾamn Al-ʾiliktruni Limuwajihat Al-Ikhtiraqat Wa Al-Hujumat Al-ʿaliyya Al-Taʿqid Lilbana Al-Tahtiyya Al-Istratajiyya [National Centre for Electronic Security to Confront Hacks and Attacks of Increased Complexity against Critical Infrastructure]’. Al-Iqtisadiyya, 27 June 2013. https://perma.cc/JMH9-R9VB.
Barakat, Muhammad. ‘Musaʿid Wazir Al-Dakhiliyya Li “Muʿalumat Wa Al-Tawthiq”: Nuharibu Milishiyyat Alʾikhwan Wa Kaʾanana Nalʿabu Shatranj [Assistant Minister of Interior for “Information and Authentication”: We Fight Brotherhood Militias as If We Are Playing Chess]’. Al-Watan, 28 February 2014. https://perma.cc/7W5X-TR9A.
Hassan, ʿAbd Al-Basir. ‘Majlis Al-Nuwab Al-Misri Yaqirru Qanun Mukafahat Al-Jarimat Al-ʾiliktruniyya [Egyptian Parliament Decides on Cybercrime Law]’. BBC News, 7 June 2018. https://perma.cc/5DWF-Y64S.
Kasab, Muhammad. ‘Sukhria Min Raqaba Al-Dakhiliyya Limauqiʿat Al-Tawassul [Sarcasm over Government Surveillance of Social Media Sites]’. Al-Masry Al-Youm, 3 June 2014. https://perma.cc/S8AP-KGAZ.
Majdi, Ahmad. ‘Khabir ʾamn Al-Muʿalumat Yutalibu Bitafʿil Al-Majlis Al-ʿali Lil-ʾamn Al-Sibrani [Cybersecurity Expert Suggests Activating the High Council for Cybersecurity]’. Mubtada, 8 August 2016. https://perma.cc/DS52-T446.
Moheet. ‘Tafkik Akbar Shabaka Satu ʾiliktruni Fi Al-Tarikh [Unravelling the Biggest Electronic Network Attack in History]’. Sayyida ʾUn Lin, 12 October 2009. https://perma.cc/V97P-C4WE.
Mzdr. ‘Tamm Al-Qabd ʿala Qarsanat Al-Bunuk Al-Amrikiyya Fi Misr [Arrests in Egypt over Piracy against the American Banks]’. Swalif Soft, 13 October 2009. https://perma.cc/MD8L-UZQJ.
Shalbi, ʾAhmad. ‘Janayat Al-Mansura Tubarriʾu 41 Mutaman Min Sariqa Milliyiyin Al-Dularat Bi 3 Bunuk ʾamrikiyya [Mansoura Court Exonerates 41 People Accused of the Theft of Millions of

Dollars from 3 American Banks]'. Al-Masry Al-Youm, 9 September 2015. https://perma.cc/FF7U-3C3B.
Shuman, Muhammad, and ʾIshraf Hazaʿ. 'Mudir Mubahith Al-ʾintarnit: Narsudu Al-ʾirhabiyyin Wa La Natajassasu ʿala Al-Muwatinin [Director of Internet Research: We Observe Terrorists and Do Not Spy on the People]'. Al-Ahram, 5 June 2014. https://perma.cc/P3UP-CXHE.
Staff Report. '"Al-Majlis Al-ʿali Lil-ʾamn Al-Sibrani" ʾam Al-Majlis Al-ʿali Lil-Raqaba? [The "High Council for Cybersecurity" or the High Council for Surveillance?]'. Al-ʿArabi Al-Jadid, 18 December 2014. https://perma.cc/M3TG-4BYC.
———. 'Al-Shura Al-Saʿudi Yudifu ʿaqubat Al-Tashhir ʾila Nizam Mukafahat Al-Jaraʾim Al-Muʿalumatiyya [Saudi Council Adds Naming and Shaming Punishment to the Cybercrime Law]'. Al-Sharq Al-ʾAwsat, 18 March 2015. https://perma.cc/4QXP-Y8JR.
———. 'Al-Sijn Wa Al-Jild Wa Al-Gharama Lithalathiniyya Shahharat Bimuwatin ʿabr Alwats ʾab [Prison, Lashes and a Fine for a Woman in Her 30s Who Insulted Another Citizen over Whats App]'. Akhbar24, 16 March 2015. https://perma.cc/QE9D-CXGH.
———. 'Aramku Alsaʿudiyya: Ikhtiraq Shabakatuna Al-ʾilitroniyya Biʾab Istahdaf Iqtisad Almamlika Wa Waqqafa Tadaffuq Al-Nuft Wa Al-Ghaz [Saudi Aramco: The Hack of Our Electronic Networks Was Aimed at the Kingdom's Economy and Stopping the Flow of Oil and Gas]'. Al-Quds Al-ʿArabi, 9 December 2012. https://perma.cc/B46P-6R26.
———. 'Hujum Khariji Istahdafa Shabakat Sharikat Aramku [External Attacks Target Aramco Company Networks]'. Al-ʿArabiyya, 9 December 2012. https://perma.cc/6DRT-LZUJ.
———. 'Inʿaqada ʾawl Ijtimaʿa Lilajnat Alkhalijiyyat Lilʾamn Al-Sibrani Bilʾimarat [The Gulf Committee for Cybersecurity Held Its First Meeting in the Emirates]'. Al-Khalij, 10 February 2017. https://perma.cc/TZL3-XDEQ.
———. 'Madha Taʿarifu ʿan Firus Shamʿun Al-Mudammir? [What Do You Know about the Destructive Shamoon Virus?]'. Al-Mowaten, 24 January 2017. https://perma.cc/RJ7F-BQL9.
———. 'Man Waraʾ Al-Hujum Alʾiliktruni ʿala ʾaramku? [Who Is behind the Electronic Attack on Aramco?]'. Al-Jazeera, 29 August 2012. https://perma.cc/JT9H-HHKE.
———. 'Rusida Mauja Thaniyya Min Hujumat Shamʿun 2 Bil-Saʿudiyya [Second Wave of Shamoon 2 Attacks Observed in Saudi Arabia]'. Al-Jazeera, 17 January 2017. https://perma.cc/F9Z3-Q73P.
———. 'Shukuk Bishaʾan Muwazzafin Saʿadan ʿala Ikhtiraq Hawasib Aramku [Doubts over Employees' Help in Hacking Aramco Computers]'. Al-ʿArab, 9 September 2012. https://perma.cc/Y8UR-WTRM.
———. 'ʾamr malaki biʾinshaʾ "al-hayaʾat al-wataniyya lil-ʾamn al-sibrani" [Royal order to create the "National Centre for Cybersecurity"]'. Al-ʿArabiyya, 1 November 2017. https://perma.cc/KFB3-9JLP.
———. 'ʾistratijiyyat Al-ʾamn Al-Sibrani Tahmi Min Al-Tahdidat Alʾiliktruniyya [Cybersecurity Strategy Protects against Electronic Threats]'. Al-ʾAnbaʾ, 3 August 2017. https://perma.cc/F4WC-77HH.
Yusif, Muhammad. 'Al-Watan Tanshuru Nus Qanun Al-Jarimat Alʾiliktruniyya ʾamam Al-Nuwab [Al Watan Publishes the Text of the Electronic Crimes Law before Parliament]'. Al-Watan, 11 May 2016. https://perma.cc/KAX8-SUQH.
ʿAbd Al-Hafiz, Ghada. 'Janayat Al-Mansura Tuʾajjilu Mahkamat Al-Muttahamin Fi Qadiyyat "Al-Qarsanat Al-ʾiliktruniyya" ʾila 2 Mayo [Mansoura Court Postpones Sentencing in the Case of "Electronic Piracy" to 2 May]'. Al-Masry Al-Youm, 6 March 2010. https://perma.cc/AV3P-6CAZ.
———. 'Tuʾajjal Mahkama 43 Shaʿaban Fi Qadiyyat Al-Qarsanat Al-ʾiliktruniyya ʾila ʾabril [Trial of 43 Youths in Electronic Piracy Case Postponed until April]'. Al-Monitor, 18 February 2011. https://perma.cc/8XNV-X9NN.
ʿAbd Al-Wahhab, Sanaʾ. 'Al-Majlis Al-ʿali Lilʾamn Al-Sibrani Yajtamiʿu Limutabiʿat ʾakhar Tatawarat "Firus Al-Fidiyya" [The High Council for Cybersecurity Meets to Follow the Latest "Ransomware" Developments]'. Al-Masry Al-Youm, 15 May 2017. https://perma.cc/4N22-65UR.
ʿAli, Khalid. 'Baʿad Ikhtifaʾ 4 Sanawat… 'shamʿun Yaʿudu Limuwajihat Al-Saʿudiyya [After Disappearing for 4 Years… Shamoon Returns to Confront Saudi Arabia]'. Sabq, 1 December 2016. https://perma.cc/QK5T-8BHY.
ʿAqili, ʾIbrahim. 'Milishiyya ʾiraniyya Waraʾ Hujumat Shamʿun [Iranian Militias behind Shamoon Attacks]'. Okaz, 25 January 2017. https://perma.cc/753U-7WZB.

Official sources

Bureau of Industry and Security (USA). '2014 Report on Foreign Policy Based Export Controls'. US Department of Commerce, 2014.

———. 'FAQs: Intrusion and Surveillance Items'. US Department of Commerce. Accessed 2 August 2017. https://perma.cc/6TRT-HM3Y.

———. 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items'. *Federal Register* 80, no. 97 (20 May 2015): 28853–63.

Burnett, Lord Justice, and Mister Justice Haddon-Cave. 'Judgement on Campaign Against the Arms Trade Application, [2017] EWHC 1726 (QB)'. Royal Courts of Justice, 10 July 2017.

Council of Europe. 'Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime'. European Treaty Series - No.185, 15 August 2018. https://perma.cc/7NQM-U764.

———. 'Convention on Cybercrime (the Budapest Convention)'. European Treaty Series - No.185, 23 November 2001.

Department for Trade and Industry. *Telecommunications Related Opportunities for UK Companies in the Kingdom of Saudi Arabia*. London: UK Government, 1988.

ENISA. 'National Cyber Security Strategy of Saudi Arabia — ENISA'. NCSS. Accessed 27 May 2017. https://perma.cc/4RW3-WUH4.

EU Commission. 'Commission Delegated Regulation (EU) No 1382/2014', 22 October 2014. https://perma.cc/R7DP-CV7G.

European Parliament. 'European Parliament Resolution on the Situation in Egypt (2014/3017)', 15 January 2015. https://perma.cc/SJ8S-RGXY.

———. 'Motion for a Resolution on Egypt (2013/2820)', 10 September 2013. https://perma.cc/5ZT7-4DQY.

Export Control Organisation. 'Consolidated List of Strategic Military and Dual-Use Items That Require Export Authorisation'. UK Government, 13 July 2017.

———. 'Export Military or Dual Use Goods, Services or Technology: Special Rules'. UK Government, 11 January 2017. https://perma.cc/RBE7-7B7B.

———. 'Open General Export Licence (Cryptographic Development)'. UK Government, 20 January 2017.

FBI. 'Operation "Phish Phry"'. FBI, 7 October 2009. https://perma.cc/LFJ5-KSDH.

Federal Bureau of Investigation (FBI). 'The Insider Threat', 10 February 2014. https://perma.cc/MF4D-FG68.

Government of Bahrain. 'Kingdom of Bahrain - EGovernment Portal Cybersecurity Strategy'. eGovernment Portal, 3 October 2017. https://perma.cc/RSL4-FPJA (ENG), https://perma.cc/NNP2-CGBJ (AR).

Government of Dubai. 'Dubai Cyber Security Strategy'. Dubai Electronic Security Center, 2017.

Government of Oman. 'Information Security - Omanuna Portal'. Omanuna, 26 March 2018. https://perma.cc/8VYS-5KSW.

———. 'Royal Decree No 12/2011 Issuing the Cyber Crime Law'. Government of Oman, 2011.

Government of Qatar. 'Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law'. Squire Patton Boggs (unofficial translation), 18 September 2014.

Government of the UAE. 'Federal Decree-Law No. (5) of 2012 On Combating Cybercrimes'. Official Gazette, Issue 540 (unofficial English translation), 13 August 2012.

Gulf Cooperation Council. 'Security Agreement Between Countries of the Gulf Cooperation Council'. GCC, 13 November 2012. https://perma.cc/3W3J-RTYM.

Human Rights Council. 'The Promotion, Protection and Enjoyment of Human Rights on the Internet'. United Nations General Assembly, A/HRC/RES/20/8, 16 July 2012.

ictQatar. 'Qatar National Cyber Security Strategy'. Government of Qatar, May 2014.

———. 'Telecommunications Law - Decree Law No.34 of 2006'. Government of Qatar, 2006.

ITU. 'ITU-IMPACT Establishes First Cybersecurity Innovation Centre for Arab Region Oman Chosen as New Regional Cyber-Hub'. Global Security Mag Online, December 2012. https://perma.cc/MF8F-GZ83.

Lane, Adam. 'Countdown to Abu Dhabi Cyber Security Forum'. utilities-me.com, 10 May 2012.

https://perma.cc/2U96-L6B5.
League of Arab States. ‘Arab Convention on Combating Information Technology Offences’. League of Arab States General Secretariat, 21 December 2010.
May, Teresa. ‘Prime Minister’s Speech to the Gulf Co-Operation Council 2016’. UK Government, 2016. https://perma.cc/PFL9-73YR.
MCIT (Egypt). ‘National ICT Strategy 2012-2017: Towards a Digital Society and Knowledge-Based Economy’. MCIT, 2012.
———. ‘Publications - Egypt’s ICT Strategy 2014 -2017’. Ministry of Communications and Information Technology, 2014. https://perma.cc/X6G3-WT3F.
MCIT (Saudi Arabia). ‘20 Government Agencies to Participate in National Information Security Program (Amen)’. Ministry of Communications and Information Technology, 17 January 2016. https://perma.cc/YE3G-MKWY.
———. ‘National Information Security Strategy’. Ministry of Communications and Information Technology, January 2011.
Mubarak, Hosni. ‘Address of H.E. Mr Mohamed Hosny Mubarak at the World Summit on the Information Society’. International Telecommunication Union, 10 December 2003. https://perma.cc/HPC2-PM8U.
National Cyber Security Center. ‘Profile - Introducing the National Cyber Security Center’. Governnment of Saudi Arabia, 2017.
National Telecom Regulatory Authority (Egypt). ‘Telecommunication Regulation Law Law No.10 of 2003’. Arab Republic of Egypt, February 2003.
TechUK. ‘Assessing Cyber-Security Export Risks’. UK Government, 19 November 2014.
Telecommunications Regulatory Authority (Oman). ‘Royal Decree No. 30/2002 Telecommunications Regulatory Act’. Government of Oman, 2003.
Telecoms Regulatory Authority (Bahrain). ‘The Telecommunications Law of the Kingdom of Bahrain’. Government of Bahrain, 23 October 2002.
———. ‘TRA Heads Bahrain’s Delegation to US-GCC Cyber Security Strategic Cooperation Forum’, 14 September 2015. https://perma.cc/2JCT-55BA.
The Arab Republic of Egypt. ‘Egypt’s Constitution of 2014’. Constituteproject.org, translated by International IDEA, 2014.
UK House of Lords Select Committee on Artificial Intelligence. ‘AI in the UK: Ready, Willing and Able?’ Report of Session 2017–19, 16 April 2018.
UK Parliament. ‘Written Statement by Secretary of State for Business, Innovation and Skills (Vince Cable) on Consolidated EU and National Arms Export Licensing Criteria’. UK Parliament, 25 March 2014.
United Nations. ‘Guiding Principles on Business and Human Rights’. HR/PUB/11/04, 2011.
US Department of Commerce. ‘Egypt - Egyptian Cybersecurity Delegation Makes a Consultative Visit’. Commercial Law Development Program, 16 September 2005. https://perma.cc/4H5W-XRDF.
US House of Representatives Subcommittee on Information Technology. ‘Transcript of Discussion “Wassenaar: Cybersecurity and Export Controls”’, 12 January 2016.
Wassenaar Arrangement Secretariat. ‘Criteria for the Selection of Dual-Use Items’. Adopted in 1994 and amended by the Plenary in 2004 and 2005, 2005. https://perma.cc/U5MZ-3JG7.

Non-official sources

Abdelaal, Mohamed. ‘Egypt’s New Cybercrime Law: Another Legislative Failure’. Jurist, 9 July 2016. https://perma.cc/HED5-X2G7.
Abdelatty, Amr. ‘Egypt’s Cybersecurity Council Prompts Privacy Concerns’. Al Monitor, 15 January 2015. https://perma.cc/D4Z7-NC9M.
Abdulla, Rasha A. ‘Egypt’s Media in the Midst of Revolution’. Carnegie Endowment for International Peace, July 2014.
Access, Colin Anderson, Electronic Frontier Foundation, Human Rights Watch, Center for Democracy and Technology, and Open Technology Institute. ‘Comments to the U.S. Department of Commerce on

Implementation of 2013 Wassenaar Arrangement Plenary Agreements', 20 July 2015.
Ackerman, Elise. 'The U.N. Fought The Internet -- And The Internet Won; WCIT Summit In Dubai Ends'. Forbes, 14 December 2012. https://perma.cc/GEL3-D7ZM.
———. 'Will A Secretive Summit In Dubai Mark The End Of The Open Internet?' Forbes, 10 December 2012. https://perma.cc/2TY7-DLKL.
ADHR. 'Dispatch: Fact vs. Myth - Bahrain Independent Commission of Inquiry (BICI)'. *Americans for Democracy & Human Rights in Bahrain* (blog), 1 August 2016. https://perma.cc/JH98-MTUN.
Ahmed, Akbar Shahid. 'Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador'. HuffPost UK, 3 June 2017. https://perma.cc/97VG-J3ZR.
Ahram Online. 'Egypt to Block Websites Linked to "Terrorism"'. Ahram Online, 17 February 2015. https://perma.cc/RLJ3-LMCR.
Aitoro, Jill. 'Q&A: Raytheon CEO on Calls for Sovereignty, Moving Past Wars of Insurgency'. Defense News, 11 July 2016. https://perma.cc/RQP7-L5P7.
Al Subaihi, Thamer. 'Supporting Qatar on Social Media a Cybercrime, Says UAE Attorney General'. The National, 7 June 2017. https://perma.cc/K7Y2-8ST5.
Al-Bawaba News. 'Symantec Announces Appointment of IMT as First Managed Security Services Partner in Saudi Arabia'. Al-Bawaba, 16 May 2004.
Al-Defaiya. 'Saudi Arabia to Host Electronic Warfare Symposium', 18 October 2013. https://perma.cc/5E6S-4HEZ.
Al-Jazeera. 'Saudi Websites Hacked by "well-Intentioned" Group', 15 August 2015. https://perma.cc/JKK3-M75B.
Al-Jazeera Investigative Unit. 'How the "dual-Use" Ruse Is Employed to Sell Spyware'. *Al-Jazeera,* 10 April 2017. https://perma.cc/SQ6E-76ZY.
———. 'Spy Merchants: Spying on Dissent through Illegal Means'. *Al-Jazeera,* 10 April 2017. https://perma.cc/2CNY-EQR2.
Alkhouri, Laith, Alex Kassirer, and Allison Nixon. 'Hacking for ISIS: The Emergent Cyber Threat Landscape'. Flashpoint, 2016.
Allen, Ian. 'Islamic State's Online Army Is a Russian Front, Says German Intelligence'. intelnews.org, 20 June 2016. https://perma.cc/QMG4-UKJ7.
Al-Saud, Naef bin Ahmed. 'A Saudi Outlook for Cybersecurity Strategies: Extrapolated from Western Experience'. *Joint Forces Quarterly*, no. 64 (2012): 75–81.
Amnesty International. 'Egypt's Plan for Mass Surveillance of Social Media an Attack on Internet Privacy and Freedom of Expression'. Amnesty International, 4 June 2014. https://perma.cc/YFY3-KTQ2.
———. 'Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal'. Amnesty International, 14 February 2017.
———. 'Qatar: New Cybercrimes Law Endangers Freedom of Expression'. Amnesty International, 18 September 2014. https://perma.cc/4ZBS-732Q.
Anderson, Colin. 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies'. Access, 2015.
Anderson, Colin, and Claudio Guarnieri. 'Bahamut, Pursuing a Cyber Espionage Actor in the Middle East'. Bellingcat, 12 June 2017. https://perma.cc/S8UW-45FU.
———. 'Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia'. Bellingcat, 27 October 2017. https://perma.cc/V57A-66MU.
Anderson, Guy. 'BAE Systems Announces Eclipse Electronic Systems Acquisition and Closure of SilverSky Deal'. *Jane's Defence Industry* 32, no. 1 (1 January 2015).
———. 'Detica to Rebrand as BAE Systems Applied Intelligence'. *Jane's Defence Industry* 31, no. 2 (1 February 2014).
Arabian Business. 'Sharjah Police to Update Surveillance Infrastructure'. ITP Business Publishing, 11 September 2014.
Arthur, Charles. 'Undersea Internet Cables off Egypt Disrupted as Navy Arrests Three'. *The Guardian,* 28 March 2013. https://perma.cc/Y5R9-ZEXC.
Atef, Maged, and Sheera Frenkel. 'Egypt Begins Surveillance Of Facebook, Twitter, And Skype On Unprecedented Scale'. BuzzFeed, 17 September 2014. https://perma.cc/P37T-6CWW.
BAE Systems. 'Managing Insider Threats'. BAE Systems | Cyber Security & Intelligence, 21 July 2016. https://perma.cc/TS94-7LYL.

BAH Press release. ‘Booz Allen Hamilton Aims to Protect Middle East’. Petroleum Africa, 20 March 2012. https://perma.cc/D27N-3JXD.
Bahrain Center for Human Rights. ‘Updates: Arrest and Detention of BCHR’s President Nabeel Rajab’. Bahrain Center for Human Rights, 8 August 2017. https://perma.cc/39UJ-KBFH.
Bahrain Watch. ‘Bahrain Government Hacked Lawyers and Activists with UK Spyware’, 7 August 2014. https://perma.cc/ZWV5-LCKB.
———. ‘The IP Spy Files: How Bahrain’s Government Silences Anonymous Online Dissent’, 1 August 2013. https://perma.cc/U4PX-JC6P.
———. ‘Uncovering a Twitter Bot Army Mobilised Against Al Jazeera’. Amantech by Bahrain Watch, Digital Defenders Partnership, 24 July 2017. https://perma.cc/39MC-W75G.
Baldwin, Clare. ‘Hackers Release Files Indicating NSA Monitored Global Bank Transfers’. *Reuters*, 15 April 2017. https://perma.cc/V2R2-N5KA.
Banker Middle East. ‘Business Defence Forum: The Compliance Front Line’. SyndiGate Media Inc., 21 November 2016.
Bartz, Diane. ‘Chinese Hackers Infiltrated Five Energy Firms: McAfee’. Reuters, 10 February 2011. https://perma.cc/75A3-TZTU.
Bassiouni, Mahmoud Cherif. ‘Report of the Bahrain Independent Commission of Inquiry’. Bahrain Independent Commission of Inquiry, 10 December 2011.
BBC. ‘How BAE Sold Cyber-Surveillance Tools to Arab States’. *BBC News*, 15 June 2017. https://perma.cc/75ZM-NXYD.
———. ‘Saudi Arabian Blogger “Flogged”’. *BBC News*, 9 January 2015. https://perma.cc/36JH-YJUS.
———. ‘Saudis Uphold Blogger’s 1,000 Lashes’. *BBC News*, 7 June 2015. https://perma.cc/5RJK-P5MF.
———. ‘UN Creates New Human Rights Body’, 15 March 2006. https://perma.cc/SUQ6-LKAQ.
Behar, Richard. ‘Inside Israel’s Secret Startup Machine’. Forbes, 11 May 2016. https://perma.cc/L7EH-8ZZ4.
Ben Hassine, Wafa. ‘The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online’. Electronic Frontier Foundation, April 2016.
Bhattacharjee, Madhuparna. ‘Cross-Border Collaborations Can Tackle Cyber Security’. Muscat Daily News, 2 April 2012. https://perma.cc/6VLC-XXQE.
BI-ME. ‘Cisco and GBM Unveil Latest UAE Security Research at GITEX 2014’, 14 October 2014. https://perma.cc/EU3X-Z9W3.
Bindiya, Thomas. ‘UAE Military To Set Up Cyber Command’. Defense World, 30 September 2014. https://perma.cc/VP7F-EEXF.
Black, Ian. ‘Bahrain Torture Report Undermines UK’s Reform Claims’. *The Guardian*, 23 November 2015. https://perma.cc/79NA-5RAX.
Boland, Rita. ‘Countries Collaborate To Counter Cybercrime’. SIGNAL Magazine, 28 July 2008. https://perma.cc/WUY2-TCT2.
Borger, Julian. ‘US Rebukes Saudi Arabia over Qatar Embargo in Reversal after Trump Comments’. *The Guardian*, 20 June 2017. https://perma.cc/PW3P-6RFX.
Bowcott, Owen. ‘UK and Saudi Arabia “in Secret Deal” over Human Rights Council Place’. *The Guardian*, 29 September 2015. https://perma.cc/9CAT-J66L.
Bumiller, Elisabeth, and Thom Shanker. ‘Panetta Warns of Dire Threat of Cyberattack on U.S.’ *The New York Times*, 11 October 2012. https://perma.cc/F5ZH-YSSV.
Burkhart, Grey, and Susan Older. ‘The Information Revolution in the Middle East and North Africa’. RAND Corporation, 2003.
Buro Jansen & Jansen. ‘Gamma Group/Louthean Nelson; Arms Dealers Pur Sang’, 19 January 2017. https://perma.cc/V6RN-7XMX.
Campbell, Duncan. ‘NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET’. The Register, 5 June 2014. https://perma.cc/PR4D-25NC.
———. ‘REVEALED: GCHQ’s BEYOND TOP SECRET Middle Eastern INTERNET SPY BASE’. The Register, 2014. https://perma.cc/K3YU-66XZ.
Caspit, Ben. ‘The Israeli-Egyptian Love Affair’. Al-Monitor, 29 February 2016. https://perma.cc/N8EH-8G42.
Cellan-Jones, Rory. ‘Divisions over Internet Governance Intensify in Dubai’. *BBC News*, 10 December 2012. https://perma.cc/9TUB-BS7D.

Chen, Adrian. ‘A Chat With the Teen Saudi Hacker Who Says He Stole a Million Israeli Credit Cards’. Gawker, 6 January 2012. https://perma.cc/9WT9-7LCH.
CISCO. ‘Cisco and GBM Outline Key Steps for Digitization to Help Middle East Organizations Become IoT Ready’, 19 October 2015. https://perma.cc/UZA5-5ACM.
Clearsky. ‘Operation Dusty Sky’, January 2016. clearskysec.com/dustysky.
———. ‘Operation Dusty Sky Part 2’, June 2016. www.clearskysec.com/dustysky2.
Comguard. ‘About Comguard’. Comguard, 2014. https://perma.cc/T55Q-K3GY.
Cutting Sword of Justice. ‘Untitled’. Pastebin.com, 15 August 2012. https://perma.cc/4KZZ-GGRF.
Dajani, Haneen. ‘UAE Expats Beware, Tough Social Media Law Could See You Deported for Saving Someone’s Photo’. The National, 19 July 2015. https://perma.cc/V4VJ-THN7.
———. ‘UAE Telecoms Regulator Defends Decision to Block Snapchat Calling’. The National, 12 April 2016. https://perma.cc/STL9-SLV5.
Deibert, Ronald J. ‘Bounding Cyber Power: Escalation and Restraint in Global Cyberspace’. Centre for International Governance Innovation, October 2013.
———. ‘Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace’. Canadian Defence and Foreign Affairs Institute, August 2012.
———. ‘Towards a Cyber Security Strategy for Global Civil Society?’ Global Information Society Watch, 2011.
Deibert, Ronald J., and Rafal Rohozinski. ‘The New Cyber Military-Industrial Complex’. The Globe and Mail, 28 March 2011. https://perma.cc/PJL9-AKGU.
DeYoung, Karen, and Ellen Nakashima. ‘UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials’. *Washington Post*, 16 July 2017. https://perma.cc/TJ8D-8ZSE.
Donaghy, Rori. ‘Falcon Eye: The Israeli-Installed Mass Civil Surveillance System of Abu Dhabi’. Middle East Eye, 28 February 2015. https://perma.cc/3WX8-XMM5.
Dourado, Eli. ‘Behind Closed Doors at the UN’s Attempted “Takeover of the Internet”’. Ars Technica, 20 December 2012. https://perma.cc/TCG3-2LST.
———. ‘Protecting the Open Internet May Require Defunding the ITU. Here’s How to Do It.’ Washington Post, 18 September 2013. https://perma.cc/H2WS-2CFP.
DubaiCityGuide. ‘Fourth International Conference on Cyber Crimes’. Dubai City Guide, 15 December 2011. https://perma.cc/9RQG-BPYS.
eGov innovation. ‘ITU-IMPACT to Hold Arab Cross-Border Cyber Drill’. Enterprise Innovation, 3 July 2012. https://perma.cc/BAY6-YHAX.
El-Guindy, Mohamed N. ‘Middle East Cyber Security Threat Report 2014’. Cybersecurity for Energy and Utilities, 25 December 2013. https://perma.cc/HB2A-DUZL.
El-Guindy, Mohamed N., and Faisal Hegazy. ‘Cybercrime Legislation in the Middle East: The Road Not Travelled’. Information Systems Security Association (ISSA), 27 February 2012. https://perma.cc/T5JL-8K45.
El-Gundy, Zeinab. ‘Founding of State Cyber-Security Body Worries Digital Rights Activists’. Ahram Online, 19 December 2014. https://perma.cc/HTB3-P897.
Enoch, Nick. ‘Hamas Hails Hack Attack against Websites of Israel’s Stock Exchange, El Al Airline and Three Banks’. Mail Online, 16 January 2012. https://perma.cc/B4UK-G9Q3.
ENP Newswire. ‘Bank of Sharjah Implements BAE Systems NetReveal’. Electronic News Publishing, 29 December 2015.
FIDH. ‘Kuwaiti Cyber Crimes Law Silences Dissent: Ongoing Prosecution of Sara Al-Drees’. Worldwide Movement for Human Rights, 12 December 2016. https://perma.cc/YR93-Q4B8.
Finfisher. ‘FinFisher - Excellence in IT Investigation’. Accessed 1 August 2017. http://www.finfisher.com/FinFisher/index.html.
Finkle, Jim. ‘Exclusive: Insiders Suspected in Saudi Cyber Attack’. *Reuters*, 7 September 2012. https://perma.cc/C5M6-WPWL.
Fisher, Phineas. ‘Hack Back! A DIY Guide’, April 2016. https://perma.cc/QZE6-55R5.
Forrester, Charles. ‘Raytheon Announces Billion-Dollar Cyber Acquisition’. *Jane’s Defence Industry* 32, no. 5 (1 May 2015).
———. ‘Raytheon Expands Cybersecurity Stable’. *Jane’s Defence Industry* 29, no. 11 (1 November 2012).

Fox-Brewster, Thomas. ‘Everything We Know About NSO Group: The Professional Spies Who Hacked IPhones With A Single Text’. Forbes, 25 August 2016. https://perma.cc/G3ZG-CL5Y.
———. ‘Is An American Company’s Technology Helping Turkey Spy On Its Citizens?’ Forbes, 25 October 2016. https://perma.cc/78HM-4D23.
Franceschi-Bicchierai, Lorenzo. ‘Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia’. Motherboard, 31 January 2018. https://perma.cc/ZR94-TANK.
———. ‘Leaked Emails Show Hacking Team Lied to Its “Rascal” Customers’. Motherboard, 14 July 2015. https://perma.cc/9VUG-Z2FJ.
Frenkel, Sheera. ‘U.S. Company Distances Itself From Egyptian Surveillance System’. BuzzFeed, 18 September 2014. https://perma.cc/7TUF-CDZH.
Fryer-Biggs, Zachary. ‘Defence Companies Try to Tackle Commercial Cyber Market’. *Jane’s Defence Industry* 32, no. 5 (1 May 2015).
———. ‘Raytheon to Buy Stonesoft’. *Jane’s Defence Industry* 32, no. 12 (1 December 2015).
———. ‘Symantec Buying Technology and Hiring Cyber Experts from Boeing’. *Jane’s Defence Industry* 32, no. 2 (1 February 2015).
Gambrell, John. ‘UAE Cyber Firm DarkMatter Slowly Steps out of the Shadows’. *Times of Israel*, 1 February 2018. https://perma.cc/CU5Y-6T8L.
Gartner. ‘Gartner Says Middle East & North Africa Information Security Spending to Reach US$1.3 Billion in 2016’, 31 October 2016. https://perma.cc/3LWW-GUGP.
Gertz, Bill. ‘Iran Renews Destructive Cyber Attacks on Saudi Arabia’. *Washington Free Beacon* (blog), 22 February 2017. https://perma.cc/CBF9-XE9M.
Gilbert, David. ‘Anonymous Knocks Saudi Government Websites Offline In Protest Against Planned Beheading And Crucifixion Of Ali Mohammad Baqir Al-Nimr’. International Business Times, 28 September 2015. https://perma.cc/6Q8Y-4DVN.
Glanz, James, and John Markoff. ‘Egypt’s Autocrats Exploited Internet’s Weaknesses’. *The New York Times*, 15 February 2011. https://perma.cc/4WVN-7G8E.
Gostev, Alexander. ‘The Flame: Questions and Answers’. Securelist GREAT (Kaspersky Lab), 28 May 2012. https://perma.cc/8Z47-U5MW.
Greenemeier, Larry. ‘How Was Egypt’s Internet Access Shut Off?’ Scientific American, 28 January 2011. https://perma.cc/T3LM-E88P.
Groll, Elias. ‘Meet the NSA’s New Data Centers: Russia, China, and Venezuela – Foreign Policy’. Foreign Policy, 31 July 2013. https://perma.cc/YLD6-LXMF.
Guerin, Orla. ‘The Shadow over Egypt’. BBC News, 23 February 2018. https://perma.cc/B5UW-PZKE.
Gulf Industry. ‘Interactive Saudi Arabia Opens Offices’. *Gulf Industry* 13, no. 2 (March 2004). https://perma.cc/HT9S-FGVP.
Hakmeh, Joyce. ‘Cybercrime and the Digital Economy in the GCC Countries’. Chatham House - The Royal Institute for International Affairs, June 2017.
Halliday, Josh. ‘UAE to Tighten BlackBerry Restrictions’. *The Guardian*, 18 April 2011. https://perma.cc/PH46-HF32.
Hamama, Mohamed. ‘Egypt’s New Cybercrime Bill Could Send You to Prison’. Mada Masr, 12 October 2016. https://perma.cc/9QGR-SUFD.
Harris, Shane. ‘U.S. Hired Dictators’ Favorite Hackers’. *The Daily Beast*, 7 July 2015. https://perma.cc/2X8H-97YQ.
Hasbini, Mohamad Amin. ‘Operation Ghoul: Targeted Attacks on Industrial and Engineering Organizations’. Securelist - GREAT (Kaspersky Lab), 17 August 2016. https://perma.cc/TEF3-VW3L.
Hau, Bill, Matt Penrose, Tom Hall, and Matias Bevilacqua. ‘M-Trends 2016 EMEA Edition’. Mandiant Consulting, June 2016.
Hawari, Walaa. ‘“60 Percent of Work Force in BAE Systems Are Saudis”’. Arab News, 15 January 2012. https://perma.cc/M85V-6NET.
Help AG. ‘About Us - the Company’. Help AG, 2016. https://perma.cc/K3MY-YKPL.
Hinck, Garrett. ‘Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research’. Lawfare, 5 January 2018. https://perma.cc/5NHM-L4FL.
Hollinger, Peggy. ‘Defence Groups Take Aim at Cyber Security’. Financial Times, 28 March 2016. https://perma.cc/AQY8-DTGQ.

Householder, Allen. ‘Like Nailing Jelly to the Wall: Difficulties in Defining “Zero-Day Exploit”’. Software Engineering Institute, Carnegie Mellon University, 7 July 2015. https://perma.cc/VQ5Y-3JMY.
Human Rights Watch. ‘Egypt: Consolidating Repression Under Al-Sisi’, 12 January 2017. https://perma.cc/65AH-JPF5.
———. ‘GCC: Joint Security Agreement Imperils Rights’. Human Rights Watch, 26 April 2014. https://perma.cc/5LLC-BXEE.
———. ‘Kuwait: Cybercrime Law a Blow to Free Speech’. Human Rights Watch, 22 July 2015. https://perma.cc/265U-VVAB.
———. ‘Oman: 3-Year Sentence for Rights Activist’. Human Rights Watch, 23 March 2015. https://perma.cc/A49P-2FJD.
———. ‘Oman: Journalists Arrested for Criticizing Judiciary’. Human Rights Watch, 5 August 2016. https://perma.cc/FX3Y-6RBR.
———. ‘Oman: Rights Routinely Trampled’. Human Rights Watch, 18 December 2014. https://perma.cc/66TQ-TDS6.
———. ‘Saudi Arabia: 15-Year Sentence for Prominent Activist’. Human Rights Watch, 7 July 2014. https://perma.cc/8QNA-8U4K.
———. ‘Saudi Arabia: Free Editor Held Under Cybercrime Law’. Human Rights Watch, 16 July 2012. https://perma.cc/3EEJ-XYXJ.
———. ‘UAE: Free Two Jailed for Criticizing Egypt’. Human Rights Watch, 15 May 2016. https://perma.cc/JJX2-RNGR.
———. ‘UAE: Investigate Attacks on Rights Defender’, 3 October 2012. https://perma.cc/K7Q8-ZV3U.
———. ‘UAE: Unfair Mass Trial of 94 Dissidents’. Human Rights Watch, 3 April 2013. https://perma.cc/43WC-NSG2.
IGF. ‘Fourth Meeting of the Internet Governance Forum Chairman’s Summary’. Internet Governance Forum, 18 November 2009.
Infosecurity. ‘Saudi Aramco Cyber Attacks a “Wake-up Call”, Says Former NSA Boss’. Infosecurity Magazine, 8 May 2014. https://perma.cc/NXT5-3J57.
Intelligence Online. ‘Abu Dhabi’s NSA and Its Helping Hands’, 5 April 2017. https://perma.cc/PTH3-AYXU.
———. ‘Mohammed Bin Nayef Pursues Cyber Ambitions’, 17 February 2016. https://perma.cc/NUJ2-CV68.
———. ‘Verint Poised to Land Major Emirates Interceptions Contract’, 18 October 2017. https://perma.cc/W6Q9-M6G5.
ISACA. ‘2016 Cybersecurity Skills Gap’. Cybersecurity Nexus, January 2016. https://perma.cc/3BZV-K2LY.
———. ‘ISACA Fact Sheet’. ISACA, January 2018. https://perma.cc/P8JT-87M7.
(ISC)^2. ‘Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate’. (ISC)^2 Blog, 17 April 2015. https://perma.cc/N7VV-XRKG.
Islamic Finance News. ‘McAfee Selects Dubai to Launch Its First Cyber Defense Center’. Contify, 3 September 2013.
ISSA. ‘ISSA Chapter Directory’. ISSA, 2016. https://perma.cc/HP3X-TNU3.
ITV. ‘Saudi Arabia Uncovered - Exposure Episode 1’. Press Centre, 9 March 2016. https://perma.cc/68PL-XQBP.
Jayoush, Kinda. ‘Cisco Sees Potential for Middle East Growth’. Reuters, 27 July 2000.
Jilani, Zaid, and Ryan Grim. ‘Hacked Emails Show Top UAE Diplomat Coordinating With Pro-Israel Think Tank Against Iran’. The Intercept, 3 June 2017. https://perma.cc/JQ5H-FNPW.
Jones, Marc Owen. ‘Saudi Royal Court Advisor Saud Al-Qahtani Is Using Bad Science to Inflame Tensions with Qatar’. Marc Owen Jones, 23 August 2017. https://perma.cc/Y4X5-WSDS.
Jones, Sam. ‘Leaked CIA Cyber Tricks May Make Us WannaCry Some More’. Financial Times, 25 May 2017. https://perma.cc/CJT6-HEP7.
Kamel, Tarek. ‘Opening Speech ICANN 33rd Meeting Opening Ceremony’. ICANN, 3 November 2008.
Karam, Souhail, and Diana Elias. ‘BlackBerry in Bid to Address Saudi Security Concerns’. *Reuters*, 8 August 2010. https://perma.cc/K9N7-J2BB.
Karr, Timothy. ‘One U.S. Corporation’s Role in Egypt’s Brutal Crackdown’. Huffington Post, 28 January

2011. https://perma.cc/2KR6-D86Q.
Kaspersky Lab. ‘From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond’. Kaspersky Lab Global Research and Analysis Team, 7 March 2017.
———. ‘Gauss: Abnormal Distribution’. Kaspersky Lab Global Research and Analysis Group, 9 August 2012.
———. ‘Gaza Cybergang, Where’s Your IR Team?’ Securelist - GREAT, 28 September 2015. https://perma.cc/B65T-WHKL.
———. ‘Shamoon the Wiper - Copycats at Work’. Securelist - GREAT, 16 August 2012. https://perma.cc/48ZN-JT7Z.
———. ‘The Desert Falcons Targeted Attacks’. Securelist - GREAT, 17 February 2015. https://perma.cc/BE9U-3NG5.
Kehl, Danielle, Andi Wilson, and Kevin Bankston. ‘Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s’. New America Foundation, Open Technology Institute, June 2015.
Khalid Negm. ‘Draft Law Concerning Electronic Crimes’. Leaked draft available on Scribd, April 2015. https://perma.cc/H4BS-VLGQ.
Kirkpatrick, David D. ‘Leaks Gain Credibility and Potential to Embarrass Egypt’s Leaders’. *The New York Times*, 12 May 2015. https://perma.cc/CNT5-RYU8.
Kirkpatrick, David D., and Sheera Frenkel. ‘Hacking in Qatar Highlights a Shift Toward Espionage-for-Hire’. *The New York Times*, 8 June 2017. https://perma.cc/4FBM-R24K.
Ko, Carol. ‘Fighting Cyber Terrorism’. Computerworld, 17 June 2008. https://perma.cc/6CZF-QG2J.
Krebs, Brian. ‘Crooks Net Millions in Coordinated ATM Heists’. *Krebs on Security* (blog), February 2013. https://perma.cc/9MSZ-QJ8F.
———. ‘Malware Spy Network Targeted Israelis, Palestinians’. *Krebs on Security* (blog), 12 November 2012. https://perma.cc/4NJT-F2SZ.
Kumar, Sheetal. ‘Cybersecurity: What’s the ITU Got to Do with It?’ Global Partners Digital, 9 July 2015. https://perma.cc/BE4P-SBQ5.
Lancaster, Tom. ‘Attacks against Israeli & Palestinian Interests - Cyber Security Updates’, 27 April 2015. https://perma.cc/4W4T-BAHZ.
Laporte-Oshiro, Catherine, and James Shires. ‘Negotiating Order in Cyberspace: Security Spirals or Trade Foundations?’ German Marshell Fund, Brussels, February 2016.
Lawson, Sean. ‘Cyber-Intifada Resource Guide: A Resource for Tracking the Intifada in Cyberspace’. The Arab Information Project, Georgetown University, 2001.
Lee, Jennifer. ‘Companies Compete to Provide Internet Veil for the Saudis’. *The New York Times*, 19 November 2001. https://perma.cc/QPQ6-PQED.
Leigh, David. ‘Offshore Company Directors’ Links to Military and Intelligence Revealed’. *The Guardian*, 28 November 2012. https://perma.cc/9MUT-9WWB.
Leigh, David, and Rob Evans. ‘BAE and the Saudis: How Secret Cash Payments Oiled £43bn Arms Deal’. *The Guardian*, 5 February 2010. https://perma.cc/2QP7-NLH2.
Leyden, John. ‘Hacking Team Mulled Stopping Ethiopia Sales – Because of Idiot g-Men’. The Register, 17 August 2015. https://perma.cc/RP3J-ULFF.
Mahdi, Wael. ‘Saudi Arabia Says Aramco Cyberattack Came From Foreign States’. *Bloomberg*, 9 December 2012. https://perma.cc/NWA4-46LT.
Mardini, Ahmed. ‘Gulf Internet: Gulf States Move to Police Cyberspace’. IPS, 4 April 1997. https://perma.cc/WGC8-3XVY.
Margaritelli, Simone. ‘How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People’, 27 July 2016. https://perma.cc/EDD3-Y9RZ.
Marlinspike, Moxie. ‘A Saudi Arabia Telecom’s Surveillance Pitch’, 13 May 2013. https://perma.cc/GT39-6JL5.
Maurer, Tim, Edin Omanovic, and Ben Wagner. ‘Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age’. New America Foundation, Open Technology Institute, Digitale Gesellschaft, Privacy International, March 2014.
Maxey, Levi. ‘Can the Law Restrain Nations in Cyberspace?’ *The Cipher Brief* (blog), 6 August 2017. https://perma.cc/WB8F-WFUA.
McAfee Labs. ‘Global Energy Cyberattacks: “Night Dragon”’. McAfee, 10 February 2011.
———. ‘Grand Theft Data: Data Exfiltration Study - Actors, Tactics and Detection’. Intel, September

2015.
———. ‘Night Dragon’. McAfee. Accessed 16 January 2018. https://perma.cc/GLD2-BJ9N.
McBride, Stephen. ‘UAE Cyber-Security Authority Unveils Policies, Standards’. ITP.net, 25 June 2014. https://perma.cc/HF7X-VFH5.
McVeigh, Karen. ‘British Firm Offered Spying Software to Egyptian Regime – Documents’. *The Guardian*, 28 April 2011. https://perma.cc/GCV9-DUJS.
MEMRI. ‘Uproar In The Gulf Following Alleged Statements By Qatari Emir Condemning Gulf States, Praising Iran, Hizbullah, Muslim Brotherhood And Hamas’. Middle East Media Research Institute Inquiry and Analysis Series No.1315, 25 May 2017. https://perma.cc/SUK8-YHDK.
Micromarketmonitor. ‘Middle East and Africa Cyber Security Market Research Report | MicroMarketMonitor.Com’, 2015. https://perma.cc/3EV9-PFDE.
Middle East Company News. ‘Cisco Advances Its Integrated Security Strategy’. AME Info, 25 February 2003.
———. ‘ECompany Signs Alliance with Symantec to Improve Internet Security in the UAE’. AME Info, 11 January 2005.
———. ‘HH Sheikh Hamed Bin Zayed Al Nahyan Launches Kustar Discovery Centre in Abu Dhabi’. AME Info, 4 July 2010.
———. ‘Kaspersky Lab Expands Its Middle East Outreach with Fusion Distribution’. AME Info, 23 January 2007.
———. ‘Kaspersky Lab Launches Arabic Edition of New Anti-Virus and Internet Security Products in Mideast’. AME Info, 17 November 2008.
———. ‘Kaspersky Lab Launches First Middle East Authorized Training Centre’. AME Info, 1 June 2009.
———. ‘Kaspersky Lab Middle East in Regional Expansion’. AME Info, 9 July 2009.
———. ‘Mohammed Bin Rashid Establishment for Young Business Leaders Company in Partnership with Symantec and Scanit’. AME Info, 23 May 2005.
———. ‘Symantec Announces Fully Arabized Education Services Tool for Improved Corporate Security’. AME Info, 5 October 2004.
———. ‘Symantec Expands Middle East Operations.’ AME Info, 13 January 2002.
Murdock, Jason. ‘BAE Systems “sold Powerful Spy Technology to Repressive Regimes” across Middle East’. International Business Times, 15 June 2017. https://perma.cc/BT7R-QQFD.
———. ‘UAE Recruiting “elite Task Force” of Cyber Experts to Build Mass Public Spying System’. International Business Times UK, 4 August 2016. https://perma.cc/E5SC-GK3B.
Mustafa, Awad. ‘UAE Leads the Way in Cyber Security’. The National, 25 February 2014. https://perma.cc/8GYK-2FTL.
Nakashima, Ellen. ‘As Cyberwarfare Heats up, Allies Turn to U.S. Companies for Expertise’. Washington Post, 22 November 2012. https://perma.cc/WNP6-UUS3.
Nasman, Carl. ‘Anonymous Hacktivist Explains Why Group Is Targeting Saudi Arabian Government’. DW.COM, 2 October 2015. https://perma.cc/WQ3Z-FZX6.
New Vision. ‘Dell to Partner up with Middle East Firms to Build Cloud Services’. 26 October 2015.
Norton Rose Fulbright. ‘Saudi Arabia Updates Cybercrime Law to Include “Naming and Shaming” Penalty’. Data Protection Report, 8 June 2015. https://perma.cc/Y287-B3N5.
Obermaier, Frederik, Henrik Moltke, Laura Poitras, and Jan Strozyk. ‘Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ’s Spying Efforts’. Sueddeutsche Zeitung, 25 November 2014. https://perma.cc/39JK-Z39V.
OCERT. ‘OCERT Event Details’, 23 October 2013. https://perma.cc/XY4F-7ZBN.
O’Leary, Jacqueline, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser. ‘Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware « Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware’. FireEye, 20 September 2017. https://perma.cc/V8SR-7KBD.
Olson, Parmy. ‘Egypt’s Internet Blackout Cost More Than OECD Estimates’. Forbes, 3 February 2011. https://perma.cc/VP9Y-8HV9.
Oxford Business Group. ‘Enhancing Saudi Arabia’s Cybersecurity Readiness’. Oxford Business Group, 29 September 2015. https://perma.cc/AAU2-RGMN.
Paganini, Pierluigi. ‘#OpNimr Anonymous Targets Saudi Websites to Stop Al-Nimr’s Crucifixion’. Security Affairs, 28 September 2015. https://perma.cc/F42P-SK3J.

Participants. ‘A Call to Cyber Norms: Discussions at Workshops, 2011 and 2012’. Harvard-MIT-University of Toronto, 2013. https://perma.cc/J884-EKXE.
Peel, Michael. ‘How the Inquiry into BAE’s Saudi Deals Was Brought to Earth’. *Financial Times*, 25 February 2007.
Perlroth, Nicole. ‘Cyberattack on Saudi Oil Firm Disquiets U.S.’ *The New York Times*, 23 October 2012. https://perma.cc/CP22-JCHM.
———. ‘How Spy Tech Firms Let Governments See Everything on a Smartphone’. *The New York Times*, 2 September 2016. https://perma.cc/3STM-RR9U.
Pironti, John. ‘The Changing Role of Security Professionals’. Infosecurity Magazine, 15 January 2013. https://perma.cc/88PD-6HCU.
Ponemon Institute LLC. ‘The State of Cybersecurity in the Oil and Gas Industry: Global’. Siemens, March 2017.
PR Newswire. ‘DarkMatter and Symantec to Provide Next-Generation Cyber Security Solutions and Services’. PR Newswire, 27 April 2016.
Prabhu, Conrad. ‘Concern over Cyber Attacks’. *Oman Daily Observer*, 20 March 2012. https://perma.cc/H69G-49R5.
Pritzker, Penny. ‘Response to Letter Regarding Implementation of the Wassenaar Arrangement “intrusion Software” and Surveillance Technology Provisions’. US Department of Commerce, 1 March 2016. https://perma.cc/9ABQ-6567.
Privacy International. ‘The Global Surveillance Industry’, July 2016.
———. ‘The President’s Men?’, February 2016.
Procera Networks. ‘Use Cases’, 2016. https://perma.cc/X8XE-SJ5Z.
Project on Middle East Democracy. ‘US Military Assistance to Egypt: Separating Fact from Fiction’. POMED, January 2018.
PwC. ‘A False Sense of Security? Cybersecurity in the Middle East’. PwC, March 2016.
———. ‘Embedding Cybersecurity into the Energy Ecosystem: An Integrated Approach to Assessing Cyber Threats and Protecting Your Assets’. PwC, February 2013.
Raff, Aviv. ‘Shamoon, a Two-Stage Targeted Attack’. *Seculert Blog on Advanced Persistent Threats and Malware* (blog), 16 August 2012. https://perma.cc/2PNQ-5XTE.
Raytheon. ‘Bursaries For Superheroes - Raytheon Funds Bursaries for Student Cyber Defenders’, 19 October 2017. https://perma.cc/CVX8-L9S4.
Raywood, Dan. ‘McAfee CTO Warns of New Combined Threat Named “Night Dragon”’. SC Media UK, 10 February 2011. https://perma.cc/QZY5-293P.
Reporters without Borders. ‘Cyber Crime Law Used Again to Silence Dissident Voices’, 1 July 2014. https://perma.cc/2M9U-S5E2.
———. ‘Enemies of the Internet’. Accessed 1 June 2017. http://12mars.rsf.org/2014-en/.
———. ‘New Cyber Crimes Law Restricts Free Expression and Targets Online Activists’, 21 January 2016. https://perma.cc/M9ZB-6VRH.
Riley, Michael, Glen Carey, and John Fraher. ‘Saudi Arabia Has Just Suffered a Series of Major Cyber Hack Attacks’. *Bloomberg*, 1 December 2016. https://perma.cc/FRK8-AV2P.
Rizvi, Sarah. ‘DarkMatter to focus on digital security at GITEX’. Channel Post MEA, 25 September 2017. https://perma.cc/GMW9-6RCP.
Rollins, Tom. ‘Egypt’s Cyber Crime Bill’. Mada Masr, 24 May 2015. https://perma.cc/A2NM-CB9L.
Rosenbach, Marcel, Hilmar Schmundt, and Christian Stöcker. ‘Source Code Similarities: Experts Unmask “Regin” Trojan as NSA Tool’. *Spiegel Online*, 27 January 2015. https://perma.cc/SEH5-YA94.
Saab, Bilal Y. ‘The Gulf Rising: Defense Industrialization in Saudi Arabia and the UAE’. Brent Scowcroft Center on International Security at the Atlantic Council, May 2014.
Saad, Ragab. ‘Egypt’s Draft Cybercrime Law Undermines Freedom of Expression’. Atlantic Council, 24 April 2015. https://perma.cc/9ATE-HNNA.
Sambridge, Andy. ‘Dubai Sets up E-Security Centre to Fight Cyber Criminals’. ITP.net, 13 June 2014. https://perma.cc/F7LX-R2VZ.
Santora, Marc. ‘In Hours, Thieves Took $45 Million in A.T.M. Scheme’. *The New York Times*, 9 May 2013. https://perma.cc/3A8A-5RG6.
Savage, John E., and Bruce W. McConnell. ‘Exploring Multi-Stakeholder Internet Governance’. EastWest Institute, January 2015.

Sengupta, Somini. ‘United Nations Chief Exposes Limits to His Authority by Citing Saudi Threat’. *The New York Times*, 9 June 2016. https://perma.cc/3XJ8-GNSK.
Shalal-Esa, Andrea. ‘Lockheed Aims to Conquer Markets Outside U.S.’ *Reuters*, 21 June 2013. https://perma.cc/Z22S-AB8G.
Silver, Vernon, and Ben Elgin. ‘Torture in Bahrain Becomes Routine with Help from Nokia Siemens’. *Bloomberg*, 23 November 2011. https://perma.cc/WT2A-XTRF.
Simms, Hannah. ‘Insider Threats Make up 74% of Business Cyber Security Incidents’. IT PRO, 22 September 2017. https://perma.cc/KYR5-GMHV.
Singer, Bill. ‘Feds Catch Their Illegal Limit In Operation Phish Phry’. Forbes, 15 May 2012. https://perma.cc/ZDL7-Z59U.
Smith, Brad. ‘The Need for a Digital Geneva Convention’. *Microsoft on the Issues* (blog), 14 February 2017. https://perma.cc/LTR3-ESKL.
Souter, David, and Abiodun Jagun. ‘Whose Summit? Whose Information Society? Developing Countries and Civil Society at the World Summit on the Information Society’. APC, 2007.
Stabe, Martin, Steve Bernard, and Marissa Oberlander. ‘The New Cyber-Industrial Complex’. *Financial Times*, 10 October 2011.
Staff Report. ‘CAIT Chief Briefs HH the Amir on National Cybersecurity Strategy - Vision to Protect Kuwait’s National Interest’. Arab Times, 31 July 2017. https://perma.cc/KTQ7-GW8G.
———. ‘Dewa Sets up 24/7 Cyber Defence Centre’. Gulf News, 17 August 2016. https://perma.cc/D3CZ-ZFZC.
———. ‘Egyptian Government Bypasses ISPs to Block Access to Websites: Telecommunications Ministry Source’. Mada Masr, 21 June 2017. https://perma.cc/9WXV-DVFG.
———. ‘India Is “ready to Use” Blackberry Message Intercept System’. *BBC News*, 11 July 2013. https://perma.cc/MJ8K-2R3F.
———. ‘Infinite Eyes in the Network: Government Escalates Attack on Secure Communication’. Mada Masr, 10 February 2017. https://perma.cc/8DJ5-SHD9.
———. ‘Liam Fox Defends Mideast Arms Sales’. The Independent, 22 February 2011. https://perma.cc/5Y7E-QUV9.
———. ‘Meet The Cyber-Industrial Complex: Private Contractors May Get $7B Windfall From Pentagon’s Cyberwar On ISIS’. International Business Times, 7 March 2016. https://perma.cc/SQ4S-8MEM.
———. ‘Omani Jailed for Insulting UAE on Whatsapp’. Al-ʿArabi Al-Jadid, 29 February 2016. https://perma.cc/2ULR-LTFQ.
———. ‘Qatar Reveals Preliminary Results of QNA Hacking Probe’. Al-Jazeera, 7 June 2017. https://perma.cc/6VVW-EGFC.
———. ‘UAE Rights Activist Ahmed Mansoor Put on Trial in Abu Dhabi’. Al-Jazeera, 18 April 2018. https://perma.cc/8MWW-JCMV.
Starlink. ‘Starlink Celebrates 10 Years as the Region’s Trusted Security Advisor’. StarLink, October 2015. https://perma.cc/H5JQ-K56W.
Stevens, Tim. ‘Norms, Epistemic Communities and the Global Cyber Security Assemblage’. *E-International Relations* (blog), 27 March 2012. https://perma.cc/8TXC-7XA7.
Stone, John. ‘Britain’s Arms Control Committee Can’t Agree What to Do about Selling Bombs to Saudi Arabia’. The Independent, 15 September 2016. https://perma.cc/QBZ8-FXYR.
Symantec. ‘Symantec to Acquire Blue Coat and Define the Future of Cybersecurity’. Symantec Press Room, 2016. https://perma.cc/38YH-NS3H.
Symantec Security Response. ‘Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance’, 24 November 2014.
———. ‘The Shamoon Attacks’, 16 August 2012. https://perma.cc/BS32-A7BW.
TeleGeography. ‘Submarine Cable Map’. http://www.submarinecablemap.com/. Accessed 16 January 2017. http://www.submarinecablemap.com/.
Tesquet, Olivier. ‘Amesys: Egyptian Trials and Tribulations of a French Digital Arms Dealer’. Telerama, 5 July 2017. https://perma.cc/L288-BMJN.
The Star. ‘Internet Security & Web Scaling from CISCO’. WorldSources Online, Inc., 10 December 1998.
Thomas, Nicki, and and Amy Dempsey. ‘Guelph-Based Software Censors the Internet in the Middle East’. *The Toronto Star*, 13 June 2011. https://perma.cc/KH8H-KXPT.

Thompson, Ben. ‘UAE Blackberry Update Was Spyware’. BBC News, 21 July 2009. https://perma.cc/97UP-3APN.
Times of Israel. ‘Israeli Government Okayed Sale of Spyware That Exploits IPhones’, 7 September 2016. https://perma.cc/62JF-CF2G.
Toumi, Habib. ‘GCC Ministers Sign Major Security Agreement’. GulfNews, 12 November 2012. https://perma.cc/5S7N-CBN5.
Trade Arabia. ‘Olton to Launch Improved Intelligence System’. Al Hilal Publishing, 24 February 2011.
Trenwith, Courtney. ‘McAfee Opens Its First Cyber Defence Centre in Dubai’. ITP.net, 3 September 2013. https://perma.cc/JER3-BWL4.
Tripputi, Christian. ‘New Reconnaissance Threat Trojan.Laziok Targets the Energy Sector’. Symantec Security Response, 30 March 2015. https://perma.cc/Z6NW-M6U9.
UAE Government News. ‘Raytheon in Talks With UAE to Make Security Deal’. Contify, 21 July 2010.
Unipath. ‘Building a Regional Cyber Partnership’. *Unipath* (blog), 20 August 2015. https://perma.cc/Q4S9-G6C5.
Unknown. ‘Out of Sight, out of Mind? Blocking Doha News in Qatar’. Journal of Middle Eastern Politics and Policy, 12 January 2017. https://perma.cc/UX6E-KMB2.
Villeneuve, Nart. ‘New Xtreme RAT Attacks US, Israel, and Other Foreign Governments’. TrendLabs Security Intelligence Blog, 14 November 2012. https://perma.cc/R5GC-7FAB.
Villeneuve, Nart, Thoufique Haq, and Ned Moran. ‘Operation Molerats: Middle East Cyber Attacks Using Poison Ivy’. FireEye, 23 August 2013. https://perma.cc/6UJT-WKZ2.
Wanjiku, Rebecca. ‘Cairo to Host ICANN Meeting in November’. CIO, 20 May 2008. https://perma.cc/NJ8X-ZH9N.
Waterman, Shaun. ‘The Wassenaar Arrangement’s Latest Language Is Making Security Researchers Very Happy’. Cyberscoop, 20 December 2017. https://perma.cc/V7PH-KJ4X.
Wax, Emily. ‘Mumbai Attackers Made Sophisticated Use of Technology’. *Washington Post*, 3 December 2008. https://perma.cc/SH9U-BT7M.
Wintour, Patrick. ‘Russian Hackers to Blame for Sparking Qatar Crisis, FBI Inquiry Finds’. *The Guardian*, 7 June 2017. https://perma.cc/3CFY-ZQ6D.
Wolff, Josephine. ‘Why Computer Science Programs Don’t Require Cybersecurity Classes’. *Slate*, 14 April 2016. https://perma.cc/CE2T-JJF5.
Wray, Richard. ‘UAE BlackBerry Ban Set to Spread throughout Gulf States’. *The Guardian*, 2 August 2010. https://perma.cc/KFA2-NHRN.
Xinhua News Agency. ‘UAE to Establish Computer Emergency Response Team’. Xinhua, 30 August 2007.
Zetter, Kim. ‘Gang of 100 Phishers Charged in U.S., Egypt’. Wired, 7 October 2009. https://perma.cc/M9R8-J49Y.
———. ‘Undersea Cables Cut; 14 Countries Lose Web -- Updated’. Wired, 19 December 2008. https://perma.cc/DE4A-856D.

Citizen Lab reports

Citizen Lab. ‘Tracking GhostNet: Investigating a Cyber Espionage Network’. Citizen Lab, 28 March 2009.
Dalek, Jakub, Ron J. Deibert, Sarah McKune, Phillipa Gill, and Adam Senft. ‘Information Controls During Military Operations The Case of Yemen’. Citizen Lab, 21 October 2015.
Dalek, Jakub, Ronald J. Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft. ‘Tender Confirmed, Rights at Risk: Verifying Netsweeper in Bahrain’. Citizen Lab, 21 September 2016.
Dalek, Jakub, and Adam Senft. ‘Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma’. Citizen Lab, 9 November 2011.
Haselton, Bennett. ‘Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE’. Citizen Lab, 28 November 2013.
Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ronald J. Deibert. ‘Bad Traffic: Sandvine’s PacketLogic Devices Used to Deploy Government Spyware in Turkey and

Redirect Egyptian Users to Affiliate Ads?' Citizen Lab, 9 March 2018.
Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune. 'Hacking Team's US Nexus'. Citizen Lab, 28 February 2014.
Marczak, Bill, and Morgan Marquis-Boire. 'From Bahrain with Love: Finfisher's Spy Kit Exposed?' Citizen Lab, 25 July 2012.
Marczak, Bill, and John Scott-Railton. 'Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents'. Citizen Lab, 29 May 2016.
———. 'The Million Dollar Dissident: NSO Group's IPhone Zero-Days Used against a UAE Human Rights Defender'. Citizen Lab, 24 August 2016.
Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. 'Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation'. Citizen Lab, 15 October 2015.
Marquis-Boire, Morgan. 'Backdoors Are Forever: Hacking Team and the Targeting of Dissent?' Citizen Lab, 10 October 2012.
Marquis-Boire, Morgan, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masishi Crete-Nishihata, Ron J. Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. 'Planet Blue Coat: Mapping Global Surveillance and Censorship Tools'. Citizen Lab, January 2013.
Marquis-Boire, Morgan, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola. 'Police Story: Hacking Team's Government Surveillance Malware'. Citizen Lab, June 2014.
Scott-Railton, John, Bill Marczak, Ramy Raoof, and Etienne Maynier. 'Nile Phish: Large Scale Phishing Campaign Targeting Egyptian Civil Society'. Citizen Lab, 2 February 2017.

Wikileaks

Wikileaks. 'Finfisher - Customers', 15 September 2014. Spy Files 4. https://perma.cc/MVB9-8VDC.
———. 'Hacking Team Email-ID 11899', 29 May 2015. https://perma.cc/NRA9-8JPA.
———. 'Hacking Team Email-ID 26180', 1 March 2015. https://perma.cc/KBT5-EPTE.
———. 'Hacking Team Email-ID 40259', 16 April 2015. https://perma.cc/2XLK-8RK5.
———. 'Hacking Team Email-ID 49934', 7 March 2015. https://perma.cc/RR6Y-N2R7.
———. 'Hacking Team Email-ID 72106', 26 March 2014. https://perma.cc/9JGB-LATM.
———. 'Hacking Team Email-ID 78759', 3 September 2013. https://perma.cc/9QGX-N942.
———. 'Hacking Team Email-ID 120169', 22 August 2014. https://perma.cc/GQ92-FFQC.
———. 'Hacking Team Email-ID 149888', 12 August 2014. https://perma.cc/QS2F-53KW.
———. 'Hacking Team Email-ID 155842', 13 October 2014. https://perma.cc/S36P-LCEX.
———. 'Hacking Team Email-ID 164478', 28 June 2014. https://perma.cc/UX4G-NNQH.
———. 'Hacking Team Email-ID 165092', 23 March 2014. https://perma.cc/KS9L-RHAP.
———. 'Hacking Team Email-ID 166153', 5 November 2013. https://perma.cc/HWK7-R897.
———. 'Hacking Team Email-ID 171363', 30 June 2014. https://perma.cc/EW6Y-8AT6.
———. 'Hacking Team Email-ID 174340', 26 May 2014. https://perma.cc/SR6E-BVM4.
———. 'Hacking Team Email-ID 432563', 30 December 2013. https://perma.cc/9PGK-CAMD.
———. 'Hacking Team Email-ID 574463', 6 May 2011. https://perma.cc/7BME-8MJU.
———. 'The Saudi Cables Doc#129897 FW: MOFA - Fireeye'. Wikileaks Forum, 12 February 2015. https://perma.cc/WKF3-KGGV.
———. 'US Cable: Skype Crackdown in Oman', 17 May 2013. https://perma.cc/XFS9-2WE7.
———. 'US Embassy Kuwait City - DHS Cybersecurity Discussions Focus on Internal Protections and Privacy'. Wikileaks Public Library of US Diplomacy, 28 October 2008. Public Library of US Diplomacy. https://perma.cc/M25S-3LN2.
———. 'US Embassy Kuwait City - Kuwait Interior Minister Sounds Alarm on Iran; Offers Assurances on GITMO Returnees and Security'. Wikileaks Public Library of US Diplomacy, 17 February 2010. Public Library of US Diplomacy. https://perma.cc/A79J-WF2E.
———. 'US Embassy Riyadh - Saudi Arabia: New Opportunities for Assistance with Naif Arab University'. Wikileaks Public Library of US Diplomacy, 31 August 2009. Public Library of US Diplomacy. https://perma.cc/FCF6-KT4Z.