2

Cybersecurity Governance in the GCC

James Shires

Department of Politics and International Relations, University of Oxford, Oxford, UK

2.1 Introduction

This chapter examines cybersecurity governance in the six states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates (UAE). It has five sections. The first highlights why the GCC is an important case study; the second gives an overview of key regional cybersecurity incidents; the third details relevant government organizations; the fourth examines strategies, laws, and standards; and the fifth analyzes the cybersecurity industry. The chapter concludes by identifying three themes: the regional *specificity* of cybersecurity governance, especially in relation to defense and telecoms; the importance of an international *image* of cybersecurity governance; and the *reinterpretation* of the scope of cybersecurity governance for political purposes.

First, a definitional note. "Governance" is a supremely agnostic term, in that it implies nothing about *who* governs, what structures or technologies are used, or the extent of their power. This is in many ways an analytical advantage, as in the following discussion I refer to governments, companies, technologies, professions, and people. Nonetheless, different academic traditions writing about governance, from those focused on "global governance"[1] to those examining it as "governmentality,"[2] agree on two things. First, governance is a power relationship which is fundamentally interactive, requiring the continual engagement of the governing, the governed, and intermediaries. Second, this relationship is flexible, in that many techniques of governance can be employed, ranging from the blunt to the fine-grained. Both characteristics appear in this chapter.

Rewired: Cybersecurity Governance, First Edition. Edited by Ryan Ellis and Vivek Mohan.

2.2 Why the GCC?

The literature on cybersecurity in International Relations predominantly focuses on "Western," liberal, democratic countries in Europe and the United States, or on their traditional "great power" competitors, Russia and China.[3] The GCC states provide a different perspective, as they are not major threats – in fact, they are strong allies of Western states – and they do not share many of the governing characteristics that are taken for granted in the cybersecurity literature.[4] The GCC countries have patriarchal systems of government, in which male members of the ruling family control key government departments and maintain influence in many private-sector organizations. The degree of consultation in government differs across the GCC: Kuwait has a relatively independent parliament, for instance, while Oman and Saudi Arabia have only nominally representational bodies.[5] Wider neo-patrimonial ties occur across and through all organizations. The social contract 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.[6] Leadership is based partly on co-option of potential threats, and partly on narratives that associate leaders with state creation, tribal authority, and Islam.[7]

Questions of cybersecurity arise within a general security environment very different from that in Europe or the United States. After ending their colonial relationship with Britain, the GCC states remained under the security umbrella of the United States for the last half century (excluding Oman, which retained British connections), with growing arms and defense cooperation since the Gulf War.[8] Domestically, the public sphere in the GCC is relatively diminished,[9] and the extensive powers of internal security agencies were magnified following the Arab Spring in 2011, with repression of protests across the GCC. The current Saudi rivalry with Iran hides extensive historic Iranian involvement in the Gulf.[10] There are several conflicts nearby: an ongoing war and humanitarian catastrophe in neighboring Yemen, where all GCC states other than Oman (and Qatar since June 2017) are in a coalition led by Saudi Arabia, and the wars in Syria and Libya, where GCC states are both actively involved and indirectly assist various parties.[11] The internal and external security situations are intertwined, with domestic concerns around Islamist extremism and Iranian interference tied to the above conflicts.

GCC states also differ from many cases used in cybersecurity analyses due to their initially ambivalent adoption of the internet. On the one hand, as GCC nations attempted to diversify from oil and gas revenues, they capitalized on high per capita income and education to attract multinational businesses, with attendant technological requirements including high-grade internet access.[12] On the other hand, internet adoption was sometimes limited outside the big cities, and has incorporated restrictions on the public sphere in keeping with a broader cautious approach to new communications technologies due to their

potential political effects.[13] The ability of the internet to affect society on a massive scale was demonstrated in the Arab Spring, when the Egyptian government resorted to a complete severance of internet connections following the January 2011 revolution,[14] and protests in the Gulf states were coordinated on social media.[15] In sum, the GCC states have become "wired for business, but not politics."[16]

Cybersecurity governance, in its unique position between two wider regional characteristics – a complex security environment and ambivalent adoption of the internet – is a key aspect of politics in the GCC. This study is therefore not only an important case for those seeking to understand cybersecurity governance, rarely examined in the literature,[17] but also highlights a crucial topic for the region more broadly.

2.3 Key Cybersecurity Incidents

The emergence of governance structures around an issue is often *reactive*, following specific events, although the form such structures take depends on the existing available conceptual and political resources. Consequently, cybersecurity governance in the GCC can only be understood within the background of key cybersecurity incidents. While the events below do not all fit easily into a single definition of cybersecurity, they have all been described within this bracket; I thus treat cybersecurity as found "in the wild." Although there is a sense in which cybersecurity incidents cannot be localized due to the global reach of the internet, regional perspectives can still be identified, with the caveat that they fit into a wider global pattern.

The first key incident relevant to the GCC was the "Stuxnet" malware, discovered in July 2010 and reportedly built by US and Israeli intelligence agencies to target a nuclear enrichment facility in Iran.[18] Stuxnet not only demonstrated that malware could have physical effects but also showed the cybersecurity industry that the Middle East was a potential market. In late 2011 and early 2012, further malware attributed to the United States and Israel was discovered,[19] and a "wiping" component from these was reverse-engineered and used on the Saudi national oil company Aramco and the Qatari company RasGas in August 2012.[20] It is difficult to overstate the impact of this attack, often referred to as Shamoon. If the US government – and by extension, the global cybersecurity community – described it as a "wake-up call,"[21] it had a rather more forceful impact for these states.[22] Despite the malware's lack of sophistication, Shamoon was quickly given the industry label of "Advanced Persistent Threat" (APT).

Following Shamoon, cybersecurity incidents in the GCC broadened substantially. Notable APTs included: Chinese espionage malware repurposed by a regional actor for political purposes[23]; malware written by a Kuwaiti that became prevalent across the region, with Arabic language support for users[24];

and specific energy-sector malware.[25,26] Leaks, "defacement," and denial of service incidents were associated with the Israel–Palestine conflict,[27,28] groups claiming affiliation with the Islamic State in Syria,[29] and broader collectives such as Anonymous.[30]

The GCC financial sector received its own wake-up call after BankMuscat in Oman and RAKBank in Qatar were compromised by a transnational criminal network in 2013, with millions withdrawn in cash.[31] Leaks became more common, including from the Saudi Ministry of Foreign Affairs[32] and Qatar National Bank.[33] Cybersecurity also became a social issue with a regional cultural dimension, following the exploitation of children and adolescents with smartphones across the region.[34] Finally, Shamoon returned in late 2016 and early 2017, again attributed to Iran.[35] The remodeled Shamoon malware used the date of the original incident as part of its wiping program, and persisted for several months. This time, more organizations were affected, including many Saudi Arabian government entities, with a temporary halt to operations at the Civil Aviation Authority.[36]

This brief overview suggests that cybersecurity incidents are deeply entangled with the regional political and security situation. Although the following sections demonstrate that a range of factors shape cybersecurity governance, it is initially catalyzed by events that both stem from and are interpreted according to their regional context.[37]

2.4 Government Organizations

The development of organizations for cybersecurity governance in the GCC must first be placed in the wider context of international internet governance. Internet governance is often described as a binary choice between liberal "multistakeholder" views, in which government, civil society, and businesses all participate,[38] and authoritarian desires for larger state sovereignty and governmental control of information flows across national borders.[39] In fact, this picture is much more complex, with a variety of approaches to internet governance in both camps.[40] The GCC states are often grouped in the latter category, due to their broader conception of security and to events at the World Congress on Information Technology (WCIT) in December 2012 in Dubai, UAE.

At this conference, a motion was proposed for the International Telecommunications Union (ITU) to take responsibility for the naming and numbering functions of the internet, as well as implementing internet security measures through state-level regulation. The initial verbal proposal was made by the host and supported by Bahrain, Saudi Arabia, Russia, and Iraq, while a written version was signed by the UAE and Saudi Arabia, with Russia and China among other signatories.[41] The proposal was widely represented in Western media as a power-grab by authoritarian regimes.[42] It is likely that

security concerns at least partially motivated this proposal, given the security focus of other standards discussed at the summit,[43] although the proposal was framed as a means to "correct historical imbalances" and "US dominance."[44]

The binary narrative of internet governance can be made more nuanced by examining the role of the ITU in establishing cybersecurity organizations in the region. Prior to ITU involvement in the GCC, public cybersecurity functions were ostensibly performed by national computer emergency response teams (CERTs).[45] The ITU had provided telecommunications (originally telegraph) standards since 1865, and first attempted to include cybersecurity in its remit through the International Multilateral Partnership Against Cyber Threats (IMPACT), created with Malaysian funding and physical location in 2008.[46] IMPACT was named the official ITU "executing arm" for cybersecurity in 2011. Throughout 2012 it was negotiating with the Omani government,[47] which agreed to pay $2 million for the first "Regional Cybersecurity Centre" in Muscat, launched officially in March 2013.[48] Along with relatively high levels of funding for the ITU from Saudi Arabia – half that of the United States, but similar to that of Russia and China[49] – there were a range of close links between the GCC and the ITU, ensuring they would support the WCIT proposal.

There were also elements of regional competition. The first regional ITU cybersecurity drill was in Jordan in July 2012, before the Oman center was established.[50] After this, the next drill was held in October 2013 – but described by the Omani press as the first one in the region.[51] Also in late 2012 and early 2013, the UAE and Saudi Arabia created national cybersecurity entities to match the Omani one: the National Electronic Security Agency in the UAE, and the National Electronic Security Centre in Saudi Arabia. Despite the announcements, they were not operational for another two years.[52] The proliferation of cybersecurity bodies, despite their initial lack of capability, highlights the importance placed by GCC governments on an international image of cybersecurity governance rather than its domestic implementation, which is explored in the next section.

I now turn to other government organizations with cybersecurity responsibilities and capabilities in the GCC. There are few public pronouncements in local ministries of defense on cyber capabilities, despite procurement of sophisticated military technologies for electronic warfare.[53] The UAE is the exception, and announced its intention to create a cyber command in September 2014. When operational, it will run "in parallel" with NESA[54]; how much this is coordination, and how much conflict, remains to be seen. The only direct GCC-level contributions to cybersecurity are a joint GCC CERT, established in 2006, and a cyber working group with the United States, established in mid-2015,[55] although the wider 2012 GCC joint security agreement covers related matters, such as information-sharing between governments.[56] As others have noted, formal GCC-level structures are often token gestures,[57] suggesting that presenting an image of cooperative cybersecurity governance and military preparedness is also a major aim of the above initiatives.

The other government organizations involved in cybersecurity are interior ministries and intelligence services. As there is little official data available, their role must be inferred from observing them in action. The Citizen Lab, a research organization based at the University of Toronto, has detailed the use of several cyber capabilities against human rights activists in the GCC. The earliest examples come from 2012, when targeted surveillance software owned at that time by Gamma Group, a multinational company with a UK subsidiary, was identified on the devices of activists in Bahrain, and similar software by Italian company Hacking Team was identified in the UAE.[58] In 2013, the Bahraini Ministry of Interior used IP address identification for Twitter accounts to prosecute activists,[59] and in 2014, Hacking Team software was also identified in the Qatif region of Saudi Arabia,[60] a Shia region with a long history of protest and violent responses by security forces.[61] More recent attempts to install monitoring software on the devices of activists and journalists have been identified in the UAE and Qatar, the former using software made by the Israeli company NSO Group.[62]

Based on the examples above, three points should be stressed. First, the distribution of targeted surveillance capability across the region is uneven: for example, Kuwait is not the focus of Citizen Lab reports, partly due to lower levels of international attention, but maybe also due to differences in intelligence techniques or suppliers.[63] Second, these capabilities are mainly provided by private companies. This led to the amendment of the Wassenaar Arrangement arms control agreement in 2013, requiring a license regime within the exporting country for such technologies.[64] Finally, the integration of these capabilities into violent and repressive security practices means that for activists, journalists, and political opponents who are imprisoned and mistreated,[65] this aspect of cybersecurity is more of a threat than any incidents listed in the preceding section. Cybersecurity governance, from the perspective of those governed, thus forms part of the coercive state mechanisms that turn devices and systems of communication into a battleground in wider political struggles.

2.5 Strategies, Laws, and Standards

The strategies, laws, and standards that constitute the policy and regulatory environment for cybersecurity 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 Mohammed 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 (well over 50% in the smaller states)

through extensive training and preferential treatment for citizens. National cybersecurity strategies (published, often in draft form, in 2013 and 2014 in all GCC states other than Kuwait) echo these wider goals, presenting an image of carefully planned cybersecurity governance to their audiences.

The two earliest and most dissimilar strategies, those of Qatar and Saudi Arabia,[66] have several interesting differences, especially given their political disputes at the time (which have since escalated).[67] First, they characterize cybersecurity and its object differently in both English and Arabic versions. Qatar uses *al-fidaʾ al-ʾiliktruni* (lit: electronic space) for cyberspace, and the loan word *al-ʾamn al-sibrani* for cybersecurity, appealing to an international audience. Saudi Arabia, on the other hand, does not describe cyberspace, instead talking about networks and connections, with the focus being on *ʾamn al-muʿalumat* (information security). While both recognize that their object has no borders or restraints, the Qatar strategy emphasizes the risks to people, companies, and the state, whereas the Saudi strategy emphasizes the cultural and economic threats of information to companies and the state, a point not made by senior Saudi figures writing in US journals.[68] Thus, even within the GCC, there are significant differences in the conceptualization of cybersecurity governance in national strategy documents.

The legal environment combines regulation of electronic financial transactions, unauthorized access to systems and data, and the use of communications technologies to send or receive information that has harmful effects. Laws concerning electronic financial transactions were first introduced in the early 2000s in the UAE and Bahrain to attract global investment, followed sporadically by the other GCC states.[69] The GCC has a disparate approach to data protection: while privacy is a right in all GCC states, the application of technical and organizational safeguards to personal data is covered by a patchwork of laws, including telecoms, health, and labor laws, as well as the penal codes and constitutions, with little personal protection.[70] Although there is little legislation against third-party provision of data services or moving organizational data between sites or countries,[71] there is a strong practical push against it in most corporations and governments.[72]

Cybersecurity legislation in the GCC has a broad scope. By mid-2015, all GCC countries had passed cybercrime legislation, which included defamation or libel (refusing truth as a defense) and wide definitions of public morals and "national unity."[73] Combined with local terrorism legislation, this increases the penalties on, and restricts freedom of, expression.[74] This is in keeping with wider censorship and historical practice, although it contradicts international human rights standards.[75] For this chapter, the relevant point is that this censorship and restriction is carried out *as cybersecurity governance*, by widening notions of cybersecurity and cybercrime. GCC governments have thus reinterpreted cybersecurity legislation to their advantage in political struggles against domestic and regional opposition.

Finally, I turn to cybersecurity standards, which enable organizations in both public and private sectors to manage cybersecurity risks. In the GCC, all national cybersecurity organizations are involved in maintaining standards such as PCI DSS and ISO27001. Oman has extensive cybersecurity policies and standards due to its role as the ITU Regional Cybersecurity Centre, mentioned above, and was ranked third in the ITU-run World Cybersecurity Index in 2014. The UAE has introduced national standards based on the US model of National Institute of Standards and Technology (NIST), although these standards overlap and compete even domestically; Dubai created its own standards and authority at the same time as Abu Dhabi introduced the nation-wide standards.[76] Implementation of these standards, whether global or local, remains problematic: a survey of GCC cybersecurity professionals in 2015 indicated that 80% are unaware of cybersecurity legislation,[77] and only two-thirds "believe their company has a security policy," to which half have "low-to-moderate adherence."[78]

To unpack this further, I draw on three surveys of ISO27001 implementation in Saudi Arabia. With low levels of overall implementation – in one 2010 study, no defense sector organizations had been certified[79] – standards were low on the list of security professionals' top problems, below personnel issues like training, expertise, or salary, and organizational ones such as management involvement.[80] One survey identified Saudi Arabian culture as a major obstacle, along with the different challenge of even identifying an organization's assets.[81] It is important to read these studies in context: they are "problem-solving" in an engineering and consultancy tradition. Viewing them through a more politically oriented lens suggests that rather than a simple lack of cybersecurity awareness, these survey responses demonstrate how cybersecurity governance in the form of global standards permeates through many organizational levels and relies on influencing behavior at the micro level. These structures encounter *indirect* resistance in the form of cultural and management problems, as well as direct resistance through lack of implementation.

2.6 The Cybersecurity Industry

In the previous sections, the focus has largely been on governments; here, I turn to the private sector. In general, Carr's analysis of public–private partnerships in cybersecurity must be altered for the GCC. While she argues that partnerships suffer from the different commercial and national interests at play,[82] here the relationship is more symbiotic. Not only do governments have several ways of influencing private-sector organizations (some overt, others based on personal relationships), but also businesses are embedded at the heart of government: national strategies are written with consultancies, and government organizations are set up with technical, advisory, and day-to-day

services provided by private companies. Furthermore, the individuals involved have no single affiliation, and move between both sides with ease.

Gartner valued the 2014 "Middle East and North Africa" cybersecurity market at just over a billion dollars, rising to 1.3 billion in 2016.[83] Other reports, although using higher values than Gartner, put the region at around 7% of the global cybersecurity market in value.[84] Unsurprisingly, health, finance, and energy sectors feature heavily in market analyses, and the UAE and Saudi Arabia 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, despite the severe effects of the collapse in oil prices in 2014–2015. The cybersecurity industry centers on large companies with a prior presence in the region, as there are significant obstacles to setting up companies in much of the GCC, although the UAE is significantly less demanding.[85] Established resellers and conglomerates channel existing economic power into the new domain, in part due to their extensive connections, but also as obligatory partners for multinational companies.

One particularly interesting example is the defense industry. Worldwide, major defense multinationals have bought specialized cybersecurity companies, creating a "cyber–military–industrial complex."[86] Regionally, the defense industry has a massive interest in the GCC states: around 10% of GDP is spent on defense, often in long-term contracts with US and UK manufacturers.[87] Often these contracts include "offsets," where the manufacturer invests in other sectors so the money does not leave the purchasing country.[88] While cybersecurity is not necessarily part of offset arrangements – being a sales target in itself – defense companies such as BAE Systems, Raytheon, and Lockheed Martin have a long history of establishing technology companies and engineering faculties in local universities as part of offset programs.[89] Overall, this structure provides a twin advantage to defense multinationals: first, they have existing military and security relationships and a trusted national security role; second, they actively create new technological industries in the GCC.

The other key sector is telecoms. This sector was quasi-liberalized in the early 2000s, with a single national entity split into two or three privatized ones; however, most still have a substantial government share. The main form of competition in the GCC is insular, as the national carriers of each country enter one another's markets, although some, such as the UAE's Etisalat, range more widely across the region. These national companies funded the undersea internet cables connecting the Gulf, and are characterized as critical information infrastructure throughout the GCC. Some, such as Etisalat and its competitor Du, have made this a commercial advantage, developing managed cybersecurity services to sell across public and private sectors.

National telecoms companies maintain strong ties with their and other GCC governments, and have two further roles, based on the content that travels

over their networks. First, they control access to encrypted communications, especially given high smartphone use. Many VOIP services are blocked, with little indication whether for profit or national security.[90] Sometimes the approach is less blunt, as in a widely reported disagreement between RIM and the UAE government over the encryption of Blackberry Messenger in 2010, which ended with RIM agreeing to certain conditions.[91] A year earlier, Etisalat had updated all Blackberry phones with a "security update," which in fact allowed third-party access to communications.[92] This not only highlights clashing interpretations of cybersecurity (a national sense of cybersecurity disguised as a users' one), but also demonstrates Etisalat's close relationship with UAE security agencies, on whose instruction this was presumably issued.

Second, national telecoms companies facilitate national monitoring and web filtering. Citizen Lab investigations in 2012 demonstrated that devices manufactured by US manufacturer Blue Coat were in all GCC countries except Oman, with McAfee's Smartfilter also in Saudi Arabia and the UAE.[93] In the UAE, technological sophistication has since increased, as a "telecommunications solutions provider" reportedly owned by an Israeli individual was contracted to install a city monitoring system in Abu Dhabi.[94] Such requirements affect foreign penetration: in Saudi Arabia, contracts for the operator Virgin Mobile were delayed to "satisfy state security concerns."[95] In Bahrain, private telecoms companies are obliged to install filtering systems, which probably led to their increased use of the commercial software Netsweeper in 2016.[96] Finally, telecoms access is useful not only for regional governments but also for strategic allies: the Snowden disclosures in 2013 indicated the existence of a Government Communications Headquarters (GCHQ) base in Oman intercepting undersea cables since 2009.[97] In sum, the telecoms sector is an essential aspect of cybersecurity governance, not only due to its advantageous industry position and gatekeeper role for new technologies but also its role in monitoring and filtering.

2.7 Conclusion

The analysis of cybersecurity governance in this chapter has been based on two premises. First, that cybersecurity should not be defined a priori, but observed "in the wild," to obtain a fuller picture of its variation in different regions. Second, that governance is fundamentally a multifaceted relation of power between those governing and those governed, which depends on many micro- and mid-level interactions involving a variety of actors. Cybersecurity governance looks different depending on perspective: for some, it is mainly technocratic and administrative, while for others it is part of political struggles and violent state actions.

Given these premises, we can identify three themes. First, *image* plays a crucial role in cybersecurity governance, in that the appearance of governance is

as important as its actions. From capturing the attention of the ITU and the competitive creation of central authorities, to the bold claims of national strategies and mixed implementation of international standards, presenting an image of successful governance is a constant concern. This presentation is predominantly to an international audience, and as such may be an attempt at deterring offensive behavior as well the result of maneuvering between elites.

Second, cybersecurity itself has been reinterpreted to fit the political situation in the region; namely, low tolerance of political expression, especially after the Arab Spring, and the use of severe criminal punishments to enforce local public speech norms on social media, both of which contravene international human rights standards. Although this has led analysts to label some GCC government organizations as "enemies of the internet,"[98] the picture must be nuanced: each country has taken different strategies, and the line they draw is often not only in opposition to a supposed "Western" notion of governance but also in opposition to other paradigms within the GCC, with Qatar, the UAE, and Saudi Arabia disagreeing strongly.

Third, the fast-growing cybersecurity industry can only be understood in the context of the specific historical and economic situation it inherits. This includes dominance by the defense industry and a close relationship between government and the telecoms sector, especially given the examples of highly sophisticated surveillance provided by their close allies in the United Kingdom and United States. While there is tension created by public–private partnerships which set commercial incentives against cybersecurity goals, the more symbiotic path described in this chapter brings with it different issues, including difficulties in stimulating local innovation. Overall, the GCC thus provides not only new lessons for cybersecurity governance but also new warnings.

Acknowlegments

An earlier version of this chapter was presented at the Oxford Cyber Studies Working Group. I thank all participants and Katharin Tai for their comments, and all remaining errors are mine.

Notes

1 Anne-Marie Slaughter, "Everyday Global Governance," *Daedalus* 132, no. 1 (2003): 83–90; Elke Krahmann, "Conceptualizing Security Governance," Cooperation and Conflict 38, no. 1 (March 1, 2003): 5–26.

2 Roger Deacon, "Strategies of Governance: Michel Foucault on Power," Theoria: A Journal of Social and Political Theory, no. 92 (1998): 113–148; Michael Dillon and Andrew Neal, "Introduction," in *Foucault on Politics, Security and War*, ed. Michael Dillon and Andrew Neal (Springer, 2015), 1–20.

3 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009); Joseph S. Nye, "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly 5, no. 4 (2011): 18; David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (Routledge, 2011); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security 38, no. 2 (October 1, 2013): 7–40; Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press, 2015).

4 For introductions, see F. Gregory Gause, *Oil Monarchies* (New York: Council on Foreign Relations Press, 1994); Rosemary Said Zahlan, *The Making of the Modern Gulf States: Kuwait, Bahrain, Qatar, the United Arab Emirates and Oman* (Ithaca: Ithaca Press, 1998); Sean Foley, *The Arab Gulf States: Beyond Oil and Islam* (Boulder: Lynne Rienner Publishers, 2010).

5 Shaul Yanai, *Political Transformation of Gulf Tribal States: Elitism & the Social Contract in Kuwait, Bahrain & Dubai, 1918-1970s* (Brighton: Sussex Academic Press, 2014), 229–236; Francis Owtram, *A Modern History of Oman: Formation of the State since 1920* (London: I.B.Tauris, 2004), 179–180; Miriam Joyce, *Bahrain from the Twentieth Century to the Arab Spring* (London: Palgrave Macmillan, 2012), 54, 113; Madawi Al-Rasheed, *A History of Saudi Arabia* (Cambridge: Cambridge University Press, 2010), 182–183.

6 Hazem Beblawi and Giacomo Luciani, eds., *The Rentier State* (Routledge, 2016), 27.

7 Andrea B. Rugh, *The Political Culture of Leadership in the United Arab Emirates* (Basingstoke: Palgrave Macmillan, 2010), 219; A. Souaiaia, *Anatomy of Dissent in Islamic Societies: Ibadism, Rebellion, and Legitimacy* (London: Palgrave Macmillan, 2013), 39–45; Christopher M. Davidson, *The United Arab Emirates: A Study in Survival* (Lynne Rienner Publishers, 2005), 70–87.

8 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), 74–76.

9 Emma C. Murphy, "Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere," International Studies Quarterly 53, no. 4 (December 1, 2009): 1148.

10 Laurence Potter, ed., *The Persian Gulf in Modern Times: People, Ports, and History* (London: Palgrave Macmillan, 2014), 11–12.

11 Taimur Khan, "UAE Joins Airstrikes on ISIL Bases in Syria," *The National*, 2014, https://www.thenational.ae/world/mena/uae-joins-airstrikes-on-isil-bases-in-syria-1.238060; Roula Khalaf and Abigail Fielding Smith, "Qatar Bankrolls Syrian Revolt with Cash and Arms," *Financial Times*, May 16, 2013; C. J. Chivers and Eric Schmitt, "In Shift, Saudis Are Said to Arm Rebels in Syria," *The New York Times*, February 25, 2013, https://www.nytimes.com/2013/02/26/world/middleeast/in-shift-saudis-are-said-to-arm-rebels-in-syria.html.

12 David Held and Kristian Ulrichsen, eds., *The Transformation of the Gulf: Politics, Economics and the Global Order* (Routledge, 2011), 9.
13 Jon W. Anderson, "Is Informationalization Good for the Middle East?" Arab Media & Society Summer, no. 18 (June 12, 2013), 2–3; Ilhem Allagui, "Internet in the Middle East: An Asymmetrical Model of Development," Internet Histories 1, no. 1–2 (January 2, 2017): 97–105.
14 Matt Richtel, "Egypt Cuts Off Most Internet and Cellphone Service," *The New York Times*, January 28, 2011, https://perma.cc/RSH4-HYDR.
15 Toby Matthiesen, *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring That Wasn't* (Stanford: Stanford University Press, 2013), 39.
16 Philip N. Howard, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam* (Oxford: Oxford University Press, 2010), 80.
17 James Andrew Lewis, "Cybersecurity and Stability in the Gulf" (CSIS, January 2014), https://perma.cc/ST48-NVGX; 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: Springer, 2016), 183–194.
18 Kim Zetter, *Countdown to Zero Day* (New York: Penguin Random House, 2014).
19 Symantec, "*W32.Duqu: The Precursor to the next Stuxnet*" (Symantec, November 23, 2011); Kaspersky Lab, "*Gauss: Abnormal Distribution*" (Kaspersky Lab, August 9, 2012).
20 Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," Survival 55, no. 2 (May 1, 2013): 81–96.
21 Infosecurity, "Saudi Aramco Cyber Attacks a 'Wake-up Call,' Says Former NSA Boss," May 8, 2014, https://perma.cc/NXT5-3J57.
22 Awad Mustafa, "UAE To Double Security Budget, Focus on Cyber," February 25, 2014, https://perma.cc/8GYK-2FTL.
23 Nart Villeneuve, Thoufique Haq, and Ned Moran, "Operation Molerats: Middle East Cyber Attacks Using Poison Ivy," *FireEye*, August 23, 2013, https://perma.cc/6UJT-WKZ2.
24 Symantec, "Simple NjRAT Fuels Nascent Middle East Cybercrime Scene," *Symantec Security Response*, March 30, 2014, https://perma.cc/3CVF-QKGP.
25 Christian Tripputi, "New Reconnaissance Threat Trojan.Laziok Targets the Energy Sector," *Symantec Security Response*, March 30, 2015, https://perma.cc/Z6NW-M6U9.
26 For earlier instances of energy sector malware targeting the Middle East, see McAfee Labs, "Global Energy Cyberattacks: 'Night Dragon'" (McAfee, February10, 2011). The high value and sensitivity of geographical research makes this industry an attractive target for commercial espionage.
27 Nick Enoch, "Hamas Hails Hack Attack against Websites of Israel's Stock Exchange, El Al Airline and Three Banks," *Mail Online*, January 16, 2012, https://perma.cc/B4UK-G9Q3.

28 This cyber conflict has a much longer history: see Sean Lawson, "Cyber-Intifada Resource Guide: A Resource for Tracking the Intifada in Cyberspace" (The Arab Information Project, Georgetown University, 2001).
29 Laith Alkhouri, Alex Kassirer, and Allison Nixon, "Hacking for ISIS: The Emergent Cyber Threat Landscape" (Flashpoint, 2016).
30 David Gilbert, "Anonymous Knocks Saudi Government Websites Offline," *International Business Times*, September 28, 2015, https://perma.cc/6Q8Y-4DVN.
31 Marc Santora, "In Hours, Thieves Took $45 Million in A.T.M. Scheme," *The New York Times*, May 9, 2013, https://perma.cc/3A8A-5RG6.
32 Waqas, "Hackers Leak Confidential Data from Saudi Ministry of Foreign Affairs! It's Crazy," *HackRead*, May 22, 2015, https://perma.cc/R923-JR9H.
33 MEE, "Qatar National Bank Allegedly Hacked, Data of 1,200 Entities Leaked," *Middle East Eye*, April 27, 2016, https://perma.cc/6TMA-VCDC.
34 BBC, "Four Jailed in Bahrain for Duping British Boys into Sex Acts," *BBC News*, April 25, 2014, https://perma.cc/V6YX-5PVN; BBC, "Sex, Honour, Shame and Blackmail in an Online World," *BBC News*, October 26, 2016, https://perma.cc/Y3JT-6FY8.
35 Kaspersky Lab, "From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond" (Kaspersky Lab, March 7, 2017).
36 Michael Riley, Glen Carey, and John Fraher, "Saudi Arabia Has Just Suffered a Series of Major Cyber Hack Attacks," *Bloomberg.Com*, December 1, 2016, https://perma.cc/FRK8-AV2P.
37 This chapter was prepared prior to the complete blockade of Qatar by Bahrain, Saudi Arabia, and the UAE in June 2017. This deep rupture in the GCC was precipitated by a cybersecurity incident: the release of a fake story on the Qatari national news channel attributed to actors associated with the UAE. There is no space to consider this incident, or its extensive implications for both cybersecurity and regional politics, in this chapter.
38 John E. Savage and Bruce W. McConnell, "Exploring Multi-Stakeholder Internet Governance" (EastWest Institute, January 2015), 4–5.
39 Paul Cornish, "Governing Cyberspace through Constructive Ambiguity," Survival 57, no. 3 (May 4, 2015), 161–165.
40 Milton Mueller, Andreas Schmidt, and Brenden Kuerbis, "Internet Security and Networked Governance in International Relations," International Studies Review 15, no. 1 (March 1, 2013): 86–104.
41 Eli Dourado, "Behind Closed Doors at the UN's Attempted 'Takeover of the Internet'," *Ars Technica*, December 20, 2012, https://perma.cc/TCG3-2LST.
42 Rory Cellan-Jones, "Divisions over Internet Governance Intensify in Dubai," *BBC News*, December 10, 2012, https://perma.cc/9TUB-BS7D.
43 Elise Ackerman, "Will A Secretive Summit In Dubai Mark The End Of The Open Internet?" *Forbes*, December 10, 2012, https://perma.cc/2TY7-DLKL.
44 Sheetal Kumar, "Cybersecurity: What's the ITU Got to Do with It?," July 9, 2015, https://perma.cc/BE4P-SBQ5.

45 CERTS were established in Qatar (2005), Saudi Arabia (2006), the UAE (2008), Oman (2010), and Bahrain (2014).
46 Rita Boland, "Countries Collaborate To Counter Cybercrime," *SIGNAL Magazine*, July 28, 2008, https://perma.cc/WUY2-TCT2. 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.Carol Ko, "Fighting Cyber Terrorism," *Computerworld*, June 17, 2008, https://perma.cc/6CZF-QG2J.
47 ITU, "ITU-IMPACT Establishes First Cybersecurity Innovation Centre for Arab Region," *Global Security Mag Online*, December 2012, https://perma.cc/MF8F-GZ83.
48 ITU, "Regional Cybersecurity Centres," 2017, https://perma.cc/VB8H-6SF3.
49 Eli Dourado, "Protecting the Open Internet May Require Defunding the ITU," *Washington Post*, September 18, 2013, https://perma.cc/H2WS-2CFP.
50 eGov innovation, "ITU-IMPACT to Hold Arab Cross-Border Cyber Drill," *Enterprise Innovation*, July 3, 2012, https://perma.cc/BAY6-YHAX.
51 OCERT, "OCERT Event Details", October 23, 2013, https://perma.cc/XY4F-7ZBN.
52 Stephen McBride, "UAE Cyber-Security Authority Unveils Policies, Standards," *ITP.Net*, June 25, 2014, https://perma.cc/HF7X-VFH5.
53 Al Defaiya, "Saudi Arabia to Host Electronic Warfare Symposium," October 18, 2013, https://perma.cc/5E6S-4HEZ.
54 Thomas Bindiya, "UAE Military To Set Up Cyber Command," *Defense World*, https://perma.cc/VP7F-EEXF.
55 TRA, "TRA Heads Bahrain's Delegation to US-GCC Cyber Security Strategic Cooperation Forum," September 14, 2015, https://perma.cc/2JCT-55BA.
56 This agreement has been described as both the culmination of long-awaited security integration (Habib Toumi, "GCC Ministers Sign Major Security Agreement," *GulfNews*, November 12, 2012, https://perma.cc/5S7N-CBN5) and as a danger to human rights across the region (Human Rights Watch, "GCC: Joint Security Agreement Imperils Rights," *Human Rights Watch*, April 26, 2014, https://perma.cc/5LLC-BXEE).
57 Michael Barnett and F. Gregory 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 (New York: Cambridge University Press, 2008), 177.
58 Bill Marczak and Morgan Marquis-Boire, "From Bahrain with Love: Finfisher's Spy Kit Exposed?" (Citizen Lab, July 25, 2012); Morgan Marquis-Boire, "Backdoors Are Forever: Hacking Team and the Targeting of Dissent?" (Citizen Lab, October 10, 2012).
59 Bahrain Watch, "The IP Spy Files: How Bahrain's Government Silences Anonymous Online Dissent," 2013, https://bahrainwatch.org/ipspy/viewreport.php.

60 Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Police Story: Hacking Team's Government Surveillance Malware" (Citizen Lab, June 2014).
61 Toby Matthiesen, *The Other Saudis: Shiism, Dissent And Sectarianism* (New York: Cambridge University Press, 2014), 101–109.
62 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, August 24, 2016); Amnesty International, "Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal" (Amnesty International, February 14, 2017).
63 Oman also receives less attention, although it probably bought Gamma's software through another company, Dreamlab: Pratap Chatterjee, "Turkmenistan and Oman Negotiated to Buy Spy Software: Wikileaks in Spy Files, *WikiLeaks Supporters Forum*, September 4, 2013, https://perma.cc/J264-JW5U.
64 Colin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies" (Access, 2015), 10–15.
65 Mahmoud Cherif Bassiouni, "Report of the Bahrain Independent Commission of Inquiry" (BICI, December 10, 2011), 285–290; Human Rights Watch, "Saudi Arabia: 7 Convicted for Facebook Postings About Protests," Human Rights Watch, June 29, 2013, https://perma.cc/39GS-52ED; Human Rights Watch, "UAE: Concerns About Muslim Brotherhood Trial," *Human Rights Watch*, November 4, 2013, https://perma.cc/DB8R-6HH3.
66 MCIT, "National Information Security Strategy" (Saudi Arabia: Ministry of Communications and Information Technology, January 2011), 4; ictQatar, "Qatar National Cyber Security Strategy" (Government of Qatar, May 2014), i. Although the Saudi strategy is dated January 2011, it was officially released in February 2013: ENISA, "National Cyber Security Strategy of Saudi Arabia," https://perma.cc/4RW3-WUH4.
67 Madawi Al-Rasheed, "Saudi-Qatar Tensions Divide GCC," *Al-Monitor*, March 6, 2014, https://perma.cc/Y597-CYZJ.
68 Naef bin Ahmed Al-Saud, "A Saudi Outlook for Cybersecurity Strategies: Extrapolated from Western Experience," Joint Forces Quarterly, no.64 (2012): 75–81.
69 Mohammed Saleh Altayar, "A Comparative Study of Anti-Cybercrime Laws in the Gulf Cooperation Council Countries," *IEEEExplore*, 2017.
70 UN-ESCWA, "Cyberlaws and Regulations for Enhancing E-Commerce" (ESCWA Cyber Legislation Digest, March 2015), 4.
71 Chad Dowle and Corey Judson, "Data Protection in United Arab Emirates," *Thomson Reuters Practical Law*, May 10, 2016, https://perma.cc/35XY-M5QF.
72 Rouda Alamir Ali, "Cloud Computing in Arab States: Legal Aspect, Facts and Horizons" (ITU Arab Regional Office, July 2016), 5.
73 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 (April 1, 2014), 12.

74 Lara-Zuzan Golesorkhi, "Cases of Contention: Activism, Social Media and Law in Saudi Arabia," Arab Media & Society, no. 20 (2015), 4–5.
75 Patrick Wintour, "UN Accuses Saudi Arabia of Using Terror Laws to Suppress Free Speech," *The Guardian*, May 4, 2017, https://perma.cc/X9LP-YTCM. This tension is complicated by the growing influence of the GCC states in defining and upholding these standards:Owen Bowcott, "UK and Saudi Arabia 'in Secret Deal' over Human Rights Council Place," *The Guardian*, September 29, 2015, https://perma.cc/9CAT-J66L; Somini Sengupta, "United Nations Chief Exposes Limits to His Authority by Citing Saudi Threat," *The New York Times*, June 9, 2016, https://perma.cc/3XJ8-GNSK.
76 Andy Sambridge, "Dubai Sets up E-Security Centre to Fight Cyber Criminals," *ITP.Net*, June 13, 2014, https://perma.cc/F7LX-R2VZ.
77 CISCO, "Cisco and GBM Outline Key Steps for Digitization to Help Middle East Organizations Become IoT Ready," October 19, 2015, https://perma.cc/UZA5-5ACM.
78 BI-ME, "Cisco and GBM Unveil Latest UAE Security Research at GITEX 2014," October 14, 2014, https://perma.cc/EU3X-Z9W3.
79 Syed Irfan Nabi, Abdulrahman A. Mirza, and Khaled Alghathbar, "Information Assurance in Saudi Organizations – An Empirical Study," in *Security Technology, Disaster Recovery and Business Continuity*, ed. Wai-chi Fang, Muhammad Khurram Khan, Kirk P. Arnett, Heau-jo Kang, and Dominik Slezak, (Springer, Berlin, Heidelberg, 2010), 24.
80 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* 2014, 1–4.
81 Belal AbuSaad, Fahad A. Saeed, Khaled Alghathbar, Bilal Khan, "Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes, and Lessons Learned," *Australian Information Security Management Conference*, January 1, 2011, 4.
82 Madeline Carr, "Public–private Partnerships in National Cyber-Security Strategies," International Affairs 92, no. 1 (January 1, 2016), 61.
83 Gartner, "Middle East & North Africa Information Security Spending to Reach US$1.3 Billion in 2016," October 31, 2016, https://perma.cc/3LWW-GUGP.
84 Micromarketmonitor, "Middle East and Africa Cyber Security Market Research Report," 2015, https://perma.cc/3EV9-PFDE.
85 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), 3.
86 Ronald J. Deibert and Rafal Rohozinski, "The New Cyber Military-Industrial Complex," *The Globe and Mail*, March 28, 2011, https://perma.cc/PJL9-AKGU.
87 Sam Perlo-Freeman, "SIPRI Background Paper: Arms Transfers to the Middle East" (SIPRI, July 2009).
88 Ron Matthews, "The UK Offset Model: From Participation to Engagement," *RUSI*, July 29, 2014.

89 Bilal Y. Saab, "The Gulf Rising: Defense Industrialization in Saudi Arabia and the UAE" (The Atlantic Council, May 2014), 32.
90 A leaked US cable suggests it is a mixture of both. Wikileaks Forum, "WikiLeaks Cable: Skype Crackdown in Oman," May 17, 2013, https://perma.cc/XFS9-2WE7.
91 Josh Halliday, "UAE to Tighten BlackBerry Restrictions," *The Guardian*, April 18, 2011, https://perma.cc/PH46-HF32.
92 Ben Thompson, "UAE Blackberry Update Was Spyware," *BBC News*, July 21, 2009, https://perma.cc/97UP-3APN.
93 Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Some Devices Wander by Mistake: Planet Blue Coat Redux" (Citizen Lab, July 9, 2013); Bennett Haselton, "Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE" (Citizen Lab, November 28, 2013).
94 Rori Donaghy, "Falcon Eye: The Israeli-Installed Mass Civil Surveillance System of Abu Dhabi," *Middle East Eye*, February 28, 2015, https://perma.cc/3WX8-XMM5.
95 Auri Aittokallio, "Virgin Mobile Launches in Saudi Arabia," *Text, Telecoms. Com* (September 30, 2014), https://perma.cc/N29W-QBCY.
96 Jakub Dalek Jakub Dalek, Ron Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft, "Tender Confirmed, Rights at Risk: Verifying Netsweeper in Bahrain" (Citizen Lab, September 21, 2016).
97 Duncan Campbell, "Revealed: GCHQ'S Beyond Top Secret Middle Eastern Internet Spy Base," *The Register* (June 3, 2014), https://perma.cc/K3YU-66XZ.
98 Reporters without Borders, "Enemies of the Internet," 2014, accessed June 1, 2017, https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf.