Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf

James Shires

Cite as: Shires, James. 2020. “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf.” In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 205-226. London: Rowman & Littlefield International.

Chapter 10

Ambiguity and Appropriation

Cybersecurity and Cybercrime in Egypt and the Gulf

James Shires

On October 4, 2018, the United Kingdom strongly denounced “reckless” and “irresponsible” cyberattacks conducted by the Russian military intelligence service against a wide range of targets, including the Organization for the Prevention of Chemical Weapons, the United Kingdom’s Foreign and Commonwealth Office, and its Defence and Science Technology Laboratory. The UK statement emphasized that these attacks were “without regard for international law or established norms,” contrasting Russian actions with the “united” approach of the United Kingdom, its allies, and the international community (UK Government 2018). The UK defence secretary even drew on language previously used to describe North Korean cyberattacks (Greenberg 2017), labeling Russia a “pariah state” (Lambert, Deutsch, and Faulconbridge 2018).

This extreme rhetoric, portraying cyberspace as a black-and-white competition between the good guys and the bad, obscures a more complicated global context. To understand the true nature of this supposed bipolar division in cyber norms, it may be instructive to turn away from the headline-grabbing (and undoubtedly illegitimate) activities of Russian intelligence agencies and to look at more complex edge cases. States in the Middle East exhibit this complexity in abundance, given the variety of conflicts and tensions in the region involving both internal struggles and international interventions. More specifically, where do Egypt and the six states of the Gulf Cooperation Council (GCC)—Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates (UAE)—fit into this picture? Despite their many differences, these states share a curious position: on the one hand, their regulations, laws, and participation in international institutions place them with Russia, China, and other proponents of cyber sovereignty; on the other, their private sector cybersecurity collaborations, intelligence relationships, and offensive cyber operations are closely aligned with the United States and Europe.

This chapter argues that this contradictory position has led to two innovations in state responses to global cyber norms. First, these states have developed deliberately *ambiguous* national cybersecurity strategies that disguise differences between domestic cybersecurity priorities and those of their international partners. Second, these states have *appropriated* international norms on cybercrime—specifically the Council of Europe's Budapest Convention of 2001—in order to counter political opposition and restrict their online public spheres through new cybercrime legislation. This chapter has three sections. The first section details the contradictory position of Egypt and the Gulf states in relation to international cyber norms. The second section examines their national cybersecurity strategies, and the third section examines their cybercrime laws. Finally, it concludes that these two innovations are closely linked: the cybersecurity practices of these states, especially their appropriation of cybercrime laws, illustrates the calculated nature of the ambiguity present in their strategy documents. Finally, one caveat is necessary: the research for this chapter was conducted up to August 2018, and so developments following this date, including a recent increase in publicly available documents, are not factored into the analysis.

A COMPLEX MIDDLE GROUND

Many scholars and policy makers lament the current state of "cyber norms," especially after the failure of the U.N. Group of Governmental Experts to agree on the application of international law in cyberspace in 2017 (Grigsby 2017). The difficulty of reaching global agreement on cyber norms is generally attributed to a bipolar division in cybersecurity governance, reflecting two opposing sets of values. On one hand, there is a group of what experts have called "like-minded" states (Kaljurand 2017). This group generally includes the United States and European countries, and it believes in an open and free Internet driven largely by global market competition with some government regulation and civil society observation, known as multistakeholderism (Savage and McConnell 2015). The second group includes Iran, Russia, and China, and prioritizes state control over national "borders" in cyberspace with strict governmental limits on content, known as cyber sovereignty (Segal 2018). These differences have been described as the cyberspace element of a resurgent Cold War, in which neoliberal and democratic structures confront information control, authoritarianism, and rule-breaking (Ignatius 2016).

In fact, this picture is much more complex, with a variety of approaches to Internet governance in both camps.[1] 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" (Carr 2015). 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 (Cornish 2015). Taking this argument further, Raymond and Denardis have argued that multistakeholderism is heterogeneous and inchoate, as administrative and regulatory bodies are routinely captured by specific coalitions of both public and private sector actors (Raymond and DeNardis 2015). 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. This section argues that Egypt and the Gulf states occupy a hybrid position in the simpler bipolar model; however, a similar argument could be made regarding Raymond and DeNardis's fivefold model.

The GCC states and Egypt are not liberal democracies. They have all—to varying degrees—adopted a position of quiet cooperation and hostile confrontation with the regional cyber powers of Israel and Iran, respectively. There are also many wider differences in their economies, societies, and access to Internet technologies. There are deep political disputes between Egypt and the GCC states, illustrated starkly by the split between Qatar and the "quartet" states—Bahrain, Egypt, Saudi Arabia, and the UAE—in June 2017, with Oman and Kuwait taking a neutral position.

Despite their differences, all these states' approaches to cyber issues exhibit some similarities with the authoritarian, cyber sovereignty-focused approach of Russia, China, and Iran. Cyber sovereignty emphasizes the strong assertion of territorial boundaries and state control over internal infrastructure, transnational connections, and content produced within or by citizens of that state. For example, Article 31 of Egypt's 2014 constitution, drafted after the 2013 coup and subsequent election of President Abdel Fattah Al-Sisi, states: "the security of information space is an integral part of the system of national economy and security. The state commits to taking the necessary measures to preserve it" (The Arab Republic of Egypt 2014). Given the wide powers allocated to military and security agencies under this constitution, and the censorship practiced under Al-Sisi, it is safe to assume that "the security of information space" *('amn al-fida' al-mu'alumati*) is defined broadly along Russian or Chinese lines.

The GCC states have similar outlooks on the control of national information, also demonstrated through broad practices of censorship (Dalek et al. 2018; Haselton 2013). Also, all these states have supported an increased role for the United Nations in cybersecurity regulation and standards (Dourado 2012). The United Nations is generally the preferred venue for proponents of cyber sovereignty because its state-only structures increase the relative power of non-Western states. In contrast, multistakeholderism also includes (mainly Western) private companies and civil society representatives. Despite occasional reports of bilateral cooperation with Russia and China—for example, Egypt's 2014 intent to work with China on combatting "cybercrimes" (*The Economic Times* 2014)—the United Nations appears to be the main forum where these states work together on cybersecurity.

But despite their embrace of cyber sovereignty over multistakeholderism, Egypt and the Gulf states work more closely with the "like-minded" states than their rivals. This is based on broader security and intelligence partnerships: for example, the United Kingdom relies on Oman for signals intelligence collection highly valued by its Five Eyes partners (Campbell 2014a), while Saudi Arabia and the UAE are approved "Third Parties," able to access some U.S. signals intelligence (Campbell 2014b). These links extend into cybersecurity, which is a key commercial and diplomatic pillar of the U.K.'s Gulf Initiative (UK Trade & Investment 2013). The UAE has allegedly discussed joint "cyber tools . . . to contain and defeat Iranian aggression" with a Washington think tank, another sign of potential cooperation in the cyber realm (Jilani and Grim 2017). More broadly, there are U.K.–Saudi Arabia agreements to develop "strategic cooperation in cybersecurity" (Foreign & Commonwealth Office 2018), and U.S.–Egypt joint military exercises including cybersecurity scenarios against a background of increased U.S. military aid (Belnap 2018; Malsin 2018). Due to these extensive associations, these states cannot simply be labeled as spoiler forces against multistakeholder proponents—a label more appropriately applied to Russia, China, and Iran.

Cybersecurity links to Western liberal democracies extend beyond state-to-state relationships, as the profile of commercial cybersecurity has risen following several significant cyberattacks (Bronk and Tikk-Ringas 2013; Krebs 2013). Private companies based in the United States and Europe sell a wide range of defensive cybersecurity solutions and cybersecurity consultancy services to most major companies and government organizations in Egypt and the Gulf, which they see as a lucrative market, while arms companies with a long-standing presence in the region offer national surveillance and offensive cyber capabilities (Shires 2018). In these ways, Egypt and the Gulf states present a challenge to bipolar models of Internet governance that presume the two sides simply form Cold War-style blocs.

These states' approach—extensive cooperation despite substantive disagreement—echoes wider contradictions between the normative and strategic components of the relationships between Egypt and the Gulf states and their international allies. In the Cold War, the oil wealth of the Gulf states and Egypt's central position in pan-Arabism and the Israel–Palestine conflict motivated the United States and Europe to work with these countries, overlooking inconsistencies with the rhetoric of worldwide democracy promotion (Chase and Hamzawy 2008). After the Cold War, joint concerns over Islamist terrorism and growing arms sales encouraged an equally muted public response to human rights violations from allied governments. Both sides have attempted to square this circle. International allies argued that influence in private was more effective than public condemnation, and that working with these regimes was more likely to bring change than breaking away from them (van Rij and Wilkinson 2018). The regimes themselves paid lip service to democracy and human rights, and activists and social movements made some genuine progress (Hosseinioun 2017).

In cybersecurity, the same puzzle presents itself. There has been no indication of opposition by the US and UK governments to the raft of new cybercrime laws. More seriously, their offensive cyber activities do not fall within the limits set both rhetorically and in practice by the United States, the United Kingdom, and other "like-minded" states, which condemn the destabilizing use of cyber tools and permit cyber espionage only for narrow national security purposes. The GCC split itself was reportedly triggered by a cyber operation carried out by contractors working for the UAE, who implanted fake text praising Iran on the website of the Qatari national news agency (DeYoung and Nakashima 2017). The leaking of private e-mails of the UAE ambassador to the United States may have been a Qatari response (Ahmed 2017). Finally, as part of the ongoing dispute between Canada and Saudi Arabia, Israel-manufactured spyware was identified on the devices of Saudi dissidents in Canada, and assessed to be controlled by the Saudi government (Hubbard and Porter 2018; Marczak et al. 2018). Egypt has conducted similar cyberattacks on journalists and civil society (Scott-Railton et al. 2017). Overall, the contradictions between cyber norms and long-standing security alliances have been left unresolved, undermining the force of the norms the United Kingdom stresses in regard to states like Russia.

This complex picture, which reflects the broader tensions in these states' historical relationships with Western democracies dating back to the Cold War, suggests that a binary understanding of global cyber norms is incomplete. Amid deep conflict over basic norms, Egypt and the GCC states have maneuvered between two poles while enjoying the tacit, if not explicit, support of both sides. This suggests that global cyber norms are much more complex—and much more entangled with traditional governance practices, diplomatic relationships, and strategic concerns—than Western officials may like to admit. More broadly, to understand the complexity of cyber norms we must look outside the framework of great power competition.

AMBIGUOUS CYBERSECURITY STRATEGIES

National strategy documents are a key element of the global cybersecurity landscape: they are a requirement of many cybersecurity maturity models, and international bodies collect and compare cybersecurity strategies from around the world. The language of these strategies can be 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" (ictQatar, May 2014, vii). Such language is easy to dismiss as mere marketing, with no significant role more broadly. Instead, I argue that national cybersecurity strategies in Egypt and the Gulf states are *ambiguous*, reflecting the contradictory position of these states in cybersecurity governance.

Ambiguity is a common attribute of international politics outside the cybersecurity arena. There are many varieties of vagueness and indeterminacy in the discourse of international politics, some of which are not deliberately cultivated; ambiguity can simply stem from lack of knowledge, time pressures, or rapidly changing circumstances (especially in cybersecurity). However, other ambiguities are entirely purposeful. In Hansen's extensive analysis of ambiguity in European arms control regulations, she notes that what Henry Kissinger described as "constructive ambiguity"—ambiguity enabling differences between parties to be bridged through the presence of several alternative meanings—generally results from heterogeneity and resistance within the negotiating parties (Hansen 2016). Cornish has even used Kissinger's phrase to describe potential avenues for dialogue between multistakeholder and cyber sovereignty proponents (Cornish 2015). In this section, I focus on a more specific version of deliberate ambiguity present in cybersecurity strategy documents: ambiguity used by *one (state) author* to disguise deviations from global norms, rather than Hansen's heterogeneous ambiguity used by many negotiating parties to reach an agreement.

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 toward 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.

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. At the time of writing in August 2018, there was 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. Although other cybersecurity strategy documents are now available, especially through the UN Cyber Policy Portal, they were not included in the following analysis. Instead, I used publicly available documents that are as close to national cybersecurity strategies as possible. The sources for this analysis are listed in table 10.1.

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" (Giles and Hagestad II 2013). However, this is too simplistic a conclusion for situations where there are many terms in play. The focus of this chapter is on shifts in the scope of cybersecurity, not whether such shifts can be captured in a binary distinction between the term "cyber" on one hand and "electronic" or "information" on the other.

Table 10.1 Documents Used to Analyze 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)

First, national cybersecurity strategies generally include only an abstract summary of the issue at stake. 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” (Government of Bahrain 2017). 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” (Government of Dubai 2017). In Saudi Arabia, the strategy aims to build “an effective and secure national information security environment (*biaʾat ʾamn al-muʿalumat*)” (MCIT [Saudi Arabia] 2011), while the National Cybersecurity Centre claims to “build a resilient and secure cyberspace that protects national and citizens’ interests” (National Cyber Security Center 2017). The generalized tone of these summaries gives no indication of the cybersecurity priorities of these states.

Given this abstract tone, the term “malicious actor” is the most prominent characterization 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 activities and disruptions . . . Dubai is a major target for malicious actors” (Government of Dubai 2017, 9). Qatar also claims that it is “an attractive target for malicious actors who seek to cause disruption and destruction” (ictQatar, 3). It is worth noting that the adjective “malicious” has several translations. In the 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 (ictQatar, 4). The latter echoes a similar description for malicious software (*barmajiyyat khabitha*). The term “malicious” thus performs a similar role in incorporating a range of cyber threats into a single term in both English and Arabic.

Interestingly, these strategies 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 Centre seeks “to realize a safe, open and stable information society” (MCIT [Saudi Arabia] 2011, iv, National Cyber Security Center 2017, 12). 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”

(Government of Dubai 2017, 7, 13). The Qatar strategy claims that their "values in cybersecurity" are to "show tolerance and respect," and embrace "the free flow of ideas and information" (ictQatar, 17). In Bahrain, the aim is to "maintain the rights and values of individuals" (Government of Bahrain 2017). This language echoes wider contests over human rights values in the region, 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 emphasizes the cultural and economic threats of information to the state, although, crucially, these qualifications are *not* made by senior Saudi figures writing in U.S. journals about the Saudi cybersecurity strategy, suggesting that such figures present a calculated portrayal of abstracted Internet rights and freedoms to their international audience (Al-Saud 2012). Other Gulf states offer similar qualifications. In Kuwait, "the strategy is primarily intended to promote the culture of cybersecurity which supports the safe and right use of the electronic space" (*Arab Times* 2017), while Qatar aims to "foster a culture of cyber security that promotes safe and appropriate use of cyberspace" (ictQatar, 17). In both cases, the ambiguity of "safe and right/appropriate" disguises significant content restrictions, discussed in the next section. Finally, the Dubai strategy states that "cyber space attacks lead to a variety of threats, such as: fraud, espionage, terrorism, violation of privacy, and defamation" (Government of Dubai 2017, 12). These last two threats mean that "careful use of social media" is a "baseline control" that "should be established, maintained and supported by Dubai individuals in their implementation," along with system updates, firewalls, and password management (Government of Dubai 2017, 25). 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.

Egypt's ICT strategy demonstrates this ambiguity clearly, partly due to its publication date in 2012, shortly after the January 2011 revolution and before the 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. On the one hand, it states that "Telecommunications Law No. 10 of 2003 . . . contains certain articles that require amendment in line with Egypt's democratic transition that will promote political openness and protect freedom of expression" (MCIT [Egypt] 2014, 9). On the other hand, it also qualifies this aim, claiming to "bring about the desired balance between the considerations of freedom as a fundamental human right and privacy considerations and national security" (MCIT [Egypt] 2014, 33). 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" (MCIT [Egypt] 2014, 33). Here the national ICT strategy incorporates both an expansive definition of national security *and* an abstract endorsement of human rights values: the ambiguity of both masks the significant extent to which Egyptian cybersecurity governance differs from U.S. and European states who adopt similar language.

On top of this ambiguity, some cybersecurity strategy documents display a contradictory orientation to international cyber norms, most relevantly the Budapest Convention on Cybercrime (treated further in the next section). 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. (Government of Oman 2018)

This statement portrays the Budapest Convention as a genuine influence, although not to the extent that Oman acceded to the convention. 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. (MCIT [Egypt] 2014, 35)

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 utilized by governments to appease international audiences, rather than being a genuine influence on their national policy.

Finally, the Saudi Arabian strategy contains a similar contradiction between domestic and international stances on cybercrime. 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. (MCIT [Saudi Arabia] 2011, 65)

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, will be more difficult" (MCIT [Saudi Arabia] 2011, 66). As in Egypt, the Saudi Arabian strategy suggests that international agreements such as the Budapest Convention have limited influence on domestic cybercrime law. However, it also acknowledges that there are substantial differences in the concept of cybercrime between domestic and international levels.

In sum, although cybersecurity strategy documents in Egypt and the Gulf states have mirrored the language of human rights and a free and open Internet, this has not been matched by these states' practices. The abstract tone and internationally oriented language of national cybersecurity strategies disguises the differences between them and their Western liberal democratic allies. Furthermore, although some of these strategy documents acknowledge the Budapest Convention on Cybercrime as an international cyber norm—suggesting a Western orientation—closer analysis suggests that this acknowledgment is calculated to appeal to an international audience, and other documents explicitly argue for deviations from this norm in favor of domestic interpretations of cybercrime. In the next section, I examine these cybercrime laws in more detail.

CYBERCRIME LAWS

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[2]—for posts made by him and others on this website (BBC 2015a; 2015b; Al-Barqawi 2015). He was sentenced to 10 years in prison and 1,000 lashes; the first 50 were carried out in January 2015, but after international protests the remainder were deferred on health grounds. While recognizing the severity of the human rights violations in this incident, this section focuses on a slightly different question: is Raʾif Badawi a cybercriminal?

Cybercrime laws were drafted between 2006 and 2018 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. I first stress that "cybercrime" is an English term with no 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 is nearly always "cybercrime."

The main international norm regarding cybercrime is the Budapest Convention on Cybercrime agreed by the Council of Europe in 2001, considered briefly in the previous section. None of the states considered here have acceded to the Budapest Convention (accession is available to nonmembers of the Council of Europe, while signature is only available to members). At the time of writing, there were sixty-four ratifications or signatures/accessions to the Convention, only two of which are in the Middle East: Tunisia and Israel (Council of Europe 2018). Consequently, this section argues that the wide definitions of cybercrime by Egypt and the Gulf states are not a "localization" of this norm, in Acharya's terms, as these states are not "norm-takers": they have not accepted it as an international norm in the first place (Acharya 2004). Instead, it is a more active *appropriation* of this norm. "Appropriation" is a term used by some norm scholars to describe changes made by states to norms more generally (Zimmerman 2017, pp. 217–222). 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.

First, it should be noted that domestic cybercrime laws emerged against the backdrop of a regional agreement on cybercrime: the Convention on Combating Information Technology Offences (*jaraʾim tiqniyyat al-muʿalumat*) by the Arab League (the Arab Convention). This convention was signed in December 2010, and it has been ratified by Egypt and all GCC states other than Saudi Arabia. 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" (Hakmeh 2017, 11). However, the key word here is "almost," as none of the articles that include political and socially controversial content in the Arab Convention (12, 14, 15 or 21) are in the Budapest Convention. The Arab Convention is thus a mixture of direct influence from the earlier text and additions that repurpose the Budapest Convention toward political speech online (Al-Tahir 2015). This is an expansion of, rather than a shift away from, an economic concept of cybercrime, as the convention also includes articles on copyright infringement, fraud, and electronic payment.

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 2018, Saudi Arabia, Oman, and the UAE all updated earlier laws while Egypt, Bahrain, Qatar, and Kuwait implemented new laws (table 10.2).

Like the Arab Convention, several scholars have recognized that these cybercrime laws expand the concept of cybercrime to cover political speech online (Hakmeh 2018). Hakmeh argues that all GCC countries other than Bahrain have "additional offences not foreseen in other legal instruments" in their cybercrime laws, and "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" (Hakmeh 2018, 9). Duffy's 2014 analysis also concludes 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 (Duffy 2014).

The updated laws all strengthen existing penalties. For example, the cybercrime law in Saudi Arabia was updated in 2015 with what was termed

Table 10.2 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

a “naming and shaming” clause for offenders, allowing a name and details of their offense to be published in local newspapers with the costs to be paid by the person convicted (Al-Sharq Al-ʾAwsat 2015). 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” (Government of Oman 2011). The updated UAE law in 2012 is one of the starkest examples, as 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. (Government of the UAE 2012)

New laws, such as the Kuwait cybercrime law, include very similar provisions to the updated laws above. Human rights organizations argued that the Kuwait law was “an effective barrier to critical political speech over the Internet” (Human Rights Watch 2015b), and “a direct assault on the right to freedom of opinion and belief and the right to freedom of expression” (Reporters without Borders 2016). Interestingly, this law had been considered even before the Arab Spring: a leaked U.S. 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” (Wikileaks 2010). The expansion of cybercrime in these laws is thus far more than localization of an existing norm: it is the active renegotiation of both cybercrime and national security.

Importantly, these cybercrime laws do not just have content provisions in their texts but have all been *used* to target political speech online. In the UAE, the cybercrime law was used in 2013 to charge the son of one of ninety-four 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 (Human Rights Watch 2013). 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 criticized the UAE and Egyptian government. In this case, the cybercrime law was used to criminalize his claims of mistreatment in an earlier trial as the posting of information “intended to damage the UAE” (Human Rights Watch 2016a). Ahmed Mansoor, a well-known dissident, was also tried under cybercrime laws (Al-Jazeera 2018). In 2016, an Omani was jailed for three years after criticizing the UAE’s conduct in the war in Yemen in a Whatsapp audio recording (Al-ʿArabi Al-Jadid 2016). After the Qatar 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 (Al Subaihi 2017).

In Saudi Arabia, the cybercrime law was also used regularly to prosecute political opposition. The liberal dissident Raʾif Badawi was sentenced under the cybercrime law in 2013 (Human Rights Watch 2012). A year later, the head of a human rights organization in Saudi Arabia was also sentenced to seven years’ imprisonment under the cybercrime law (Reporters without Borders 2014). In 2015, a lawyer who had represented Raʾif Badawi, and who founded the rights organization Saudi Monitor for Human Rights, was sentenced to fifteen years imprisonment for a range of offenses, including some under the new cybercrime law (Human Rights Watch 2014a). Other lawyers confirmed the use of the cybercrime law to prosecute the “spreading of rumours” over Twitter in 2017 (Al-Barqawi 2017). Most recently, in October 2018, the Saudi Public Prosecution reiterated their willingness to use the provisions against spreading rumors in the updated cybercrime law in an oblique reference to the alleged murder of Saudi journalist Jamal Khashoggi by the Saudi government in its Turkish consulate (Saudi Gazette 2018).

Kuwait’s cybercrime law was used in 2016 to charge a blogger who criticized the emir (FIDH 2016). 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 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 (Rajab 2016). His charges included “insulting a neighbouring country” in relation to Saudi Arabia (Bahrain Center for Human Rights 2017). 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 an older criminal offense—insulting the Sultan—rather than under the cybercrime law (Human Rights Watch 2014b). In 2015, a government critic was sentenced to three years in prison for critical blog posts under the cybercrime law (Human Rights Watch 2015a). The editor of a politically independent newspaper in Oman, Al-Zaman, was charged under the cybercrime law after an article that criticized the judiciary in 2016 (Human Rights Watch 2016b). The newspaper was shut down a year later. I identified no instances of Qatar’s cybercrime law being used to suppress political opposition. However, human rights organizations highlight risks of this law through the example of a poet sentenced to fifteen years in prison in 2013 for indirectly criticizing the ruling family (Amnesty

International 2014). This poet, Muhammad Rashid Al-Ajami, was pardoned in 2016.

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 (MCIT [Egypt] 2014, 35). At least three further drafts have been proposed since the June 2013 coup, in April 2015, May 2016, and June 2018 (Yusif 2016; Negm 2015). One of the main sponsors of the 2015 draft, Minister for Communications and Information Technology Khalid Negm, claimed that it was in part prompted by the Arab Convention (Saad 2015). 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 (Abdelaal 2016). The latest draft was approved by parliament in June 2018 (Hassan 2018) and passed into law in August 2018 (Salama 2018). It is not included in the analysis here, although its provisions appear similar. Criticism of the law has focused on its broad definition of websites subject to censorship, including any that "threaten national security or expose the nation's security or economy to risk" (Article 7) (ʿAli 2018). Critics have also pointed to heavy punishments for privacy infringements of public figures, penetration testing practices by security experts, and high data management burdens on ISPs, despite insistences by officials that these are unintended or at least limited (El-Gundy 2018).

Overall, Egyptian law follows the expansive definitions of cybercrime in the other laws above (Miller 2018). Due to the recent approval of this law, Egypt has no cybercrime prosecutions at the time of writing. However, as Ben Hassine argues, Egypt already uses a variety of anti-terror and anti-protest laws to control online political activity (Ben Hassine 2016). The anti-protest laws are especially successful in this aim, as encouraging or inciting people to protest online is a more serious offense 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 (Abdulla 2014). It also highlights the violent responses of security forces to later protests, including the massacre of at least 700 people at Rabiʿa Square in 2013, and the regular disappearance and torture of activists and protesters since (Guerin 2018).

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. This innovation is important for the global development of cyber norms because it demonstrates how states that are not "norm-takers" (who did not sign up to the Budapest Convention) nonetheless incorporate such norms into their practices in a strategic maneuver, signaling their alignment with the norm through national strategy documents and then deviating from the norm in their domestic laws.

CONCLUSION

This chapter has argued that the emergence of cyber norms in Egypt and the Gulf states is characterized by ambiguity and appropriation. First, I argued that these states occupy a complex position in international cybersecurity governance, with both strong security ties to multistakeholder proponents in the United States and Europe and support for cyber sovereignty measures in multilateral forums. Second, these states' cybersecurity strategy documents accommodate the contradictions of this position by adopting an abstract and *ambiguous* description of cybersecurity threats and human rights values designed for international consumption. Although this ambiguous tone is partly a reflection of the many uses and causes of ambiguity more generally in international politics, in this case it also disguises the differences in conceptions of cybersecurity and cybercrime between these states and their international allies. Third, in the turbulent political situation after the Arab Spring, cybercrime laws and regional agreements across Egypt and the GCC *appropriated* the concept of cybercrime to provide an additional means to criminalize political speech online in an already restricted public sphere. These two innovations are closely linked: the cybersecurity practices of these states, especially their appropriation of cybercrime laws, illustrates the calculated nature of the ambiguity present in their strategy documents.

Both ambiguity and appropriation are innovations in state responses to the development of global cyber norms that could be analyzed in comparative perspective elsewhere. Future work could compare the production of ambiguity and appropriation in other regions with similar contradictory positions in global cybersecurity governance or test the logic of the argument presented here by exploring whether such maneuvers take place in states without such contradictory pressures. This chapter has thus provided an original contribution to the study of cyber norms, based on a rich empirical analysis of an important and largely unstudied region in cybersecurity. It highlights how states outside the cyber "great powers" have reached novel horizons in their sophisticated engagement with cyber norms, as—through their embrace of ambiguity and appropriation—these states participate in the constant undermining and redefining of responsible behavior itself.

NOTES

1. Daniel W. Drezner, “The Global Governance of the Internet: Bringing the State Back In,” *Political Science Quarterly* 119, no. 3 (2004): 477–498; 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; Roger Hurwitz, “The Play of States: Norms and Security in Cyberspace,” *American Foreign Policy Interests* 36, no. 5 (September 3, 2014), p. 328.

2. 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.

REFERENCES

Abdelaal, Mohamed. 2016. “Egypt’s New Cybercrime Law: Another Legislative Failure”. *Jurist*, July 9, 2016. https://perma.cc/HED5-X2G7.

Abdulla, Rasha A. 2014. “Egypt’s Media in the Midst of Revolution”. Carnegie Endowment for International Peace, July 2014.

Acharya, Amitav. 2004. “How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism”. *International Organization*, 58(2): 239–275.

Al-Barqawi, ʿAbdallah. 2017. “Mutalabat Bimuʿaqaba Murawaji Shaʾiʿat ‘Al-Qurarat’ ʿabr Muwaqiʿa Al-Tawassul [Demands to Punish the Promotion of ‘Low’ Rumours on Social Media]”. *Sabq*, November 18, 2017. https://perma.cc/5K8R-SV5G.

———. 2015. “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*, January 9, 2015. https://perma.cc/Q99Y-5F39.

Al Subaihi, Thamer. 2017. “Supporting Qatar on Social Media a Cybercrime, Says UAE Attorney General”. *The National*, June 7, 2017. https://perma.cc/K7Y2-8ST5.

Al-Saud, Naef bin Ahmed. 2012. “A Saudi Outlook for Cybersecurity Strategies: Extrapolated from Western Experience”. *Joint Forces Quarterly*, 64: 75–81.

Al-Tahir, Muhammad. 2015. “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]*, March 12, 2015. https://perma.cc/DUB8-6END.

ʿAli, ʾIman. 2018. “Nanshura Al-Nus Al-Kamil Liqanun Mukafihat Jaraʾim Al-ʾintarnat Baʿad Tasdiq Al-Raʾis Al-Sisi ʿalaihi [We Publish the Complete Text of the Law against Internet Crimes After the Ratification of President Al-Sisi]”. *Al-Masry Al-Yaum*, August 19, 2018. https://perma.cc/89P6-KZJ7.

Amnesty International. 2014. “Qatar: New Cybercrimes Law Endangers Freedom of Expression”. Amnesty International, September 18, 2014. https://perma.cc/4ZBS-732Q.

Bahrain Center for Human Rights. 2017. “Updates: Arrest and Detention of BCHR’s President Nabeel Rajab”. Bahrain Center for Human Rights, August 8, 2017. https://perma.cc/39UJ-KBFH.

BBC. 2015. “Saudi Arabian Blogger ‘Flogged’”. *BBC News*, January 9, 2015. https://perma.cc/36JH-YJUS.

Belnap, Jeffrey Dallin. 2018. “Bright Star Command Post Exercise Pursues Strategic Partnership”. *U.S. Army Central*, September 15, 2018. https://perma.cc/3GPY-C2CN.

Ben Hassine, Wafa. 2016. “The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online”. Electronic Frontier Foundation, April 2016.

Carr, Madeline. 2015. “Power Plays in Global Internet Governance”. *Millennium* 43(2): 640–659.

Cornish, Paul. 2015. “Governing Cyberspace Through Constructive Ambiguity”. *Survival* 57(3): 153–176.

Council of Europe. 2018. “Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime”. European Treaty Series—No.185, August 15, 2018. https://perma.cc/7NQM-U764.

Dalek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, John Penney, Adam Senft, and Ronald J. Deibert. 2018. “Planet Netsweeper”. Citizen Lab, April 25, 2018.

Dourado, Eli. 2012. “Behind Closed Doors at the UN’s Attempted ‘Takeover of the Internet’”. *Ars Technica*, December 20, 2012. https://perma.cc/TCG3-2LST.

Drezner, Daniel W. 2004. “The Global Governance of the Internet: Bringing the State Back In”. *Political Science Quarterly*, 119(3): 477–498.

Duffy, Matt. 2014. “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(1): 1.

El-Gundy, Zeinab. 2018. “Q&A: Egypt’s New Cybercrime Law ‘Not about Putting Barriers on the Internet’”. *Ahram Online*, August 20, 2018. https://perma.cc/QA7T-EFUR.

FIDH. 2016. “Kuwaiti Cyber Crimes Law Silences Dissent: Ongoing Prosecution of Sara Al-Drees”. *Worldwide Movement for Human Rights*, December 12, 2016. https://perma.cc/YR93-Q4B8.

Foreign & Commonwealth Office. 2018. “United Kingdom-Saudi Arabia Joint Communiqué”. GOV.UK, March 10, 2018. https://perma.cc/R9C7-LZVC.

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

Government of Bahrain. 2017. “Kingdom of Bahrain—EGovernment Portal Cybersecurity Strategy”. eGovernment Portal, October 3, 2017. https://perma.cc/RSL4-FPJA (ENG), https://perma.cc/NNP2-CGBJ (AR).

Government of Dubai. 2017. “Dubai Cyber Security Strategy”. Dubai Electronic Security Center.

Government of Oman. 2011. “Royal Decree No 12/2011 Issuing the Cyber Crime Law”. Government of Oman.

———. 2018. “Information Security—Omanuna Portal”. Omanuna, 26 March 2018. https://perma.cc/8VYS-5KSW.

Government of the UAE. 2012. “Federal Decree-Law No. (5) of 2012 On Combating Cybercrimes”. *Official Gazette*, Issue 540 (unofficial English translation), 13 August 2012.

Greenberg, Andy. 2017. “North Korea’s Sloppy, Chaotic Cyberattacks Also Make Perfect Sense”. *Wired*, June 15, 2017. https://perma.cc/A5QK-PHPH.

Guerin, Orla. 2018. “The Shadow over Egypt”. *BBC News*, 23 February 2018. https://perma.cc/B5UW-PZKE.

Hakmeh, Joyce. 2017. “Cybercrime and the Digital Economy in the GCC Countries”. Chatham House—The Royal Institute for International Affairs, June 2017.

———. 2018. “Cybercrime Legislation in the GCC Countries—Fit for Purpose?” Chatham House—The Royal Institute for International Affairs, July 2018.

Hansen, Susanne Therese. 2016. “Taking Ambiguity Seriously: Explaining the Indeterminacy of the European Union Conventional Arms Export Control Regime”. *European Journal of International Relations*, 22(1): 192–216.

Hassan, ʿAbd Al-Basir. 2018. “Majlis Al-Nuwab Al-Misri Yaqirru Qanun Mukafahat Al-Jarimat Al-ʾiliktruniyya [Egyptian Parliament Decides on Cybercrime Law]”. *BBC News*, June 7, 2018. https://perma.cc/5DWF-Y64S.

Hubbard, Ben, and Catherine Porter. 2018. “Saudi Arabia Escalates Feud With Canada Over Rights Criticism”. *The New York Times*, October 10, 2018. https://perma.cc/8H5W-MGGD.

Human Rights Watch. 2012. “Saudi Arabia: Free Editor Held Under Cybercrime Law”. *Human Rights Watch*, July 16, 2012. https://perma.cc/3EEJ-XYXJ.

———. 2013. “UAE: Unfair Mass Trial of 94 Dissidents”. *Human Rights Watch*, April 3, 2013. https://perma.cc/43WC-NSG2.

———. 2014a. “Saudi Arabia: 15-Year Sentence for Prominent Activist”. *Human Rights Watch*, July 7, 2014. https://perma.cc/8QNA-8U4K.

———. 2014b. “Oman: Rights Routinely Trampled”. *Human Rights Watch*, December 18, 2014. https://perma.cc/66TQ-TDS6.

———. 2015. “Kuwait: Cybercrime Law a Blow to Free Speech”. *Human Rights Watch*, July 22, 2015. https://perma.cc/265U-VVAB.

———. 2016. “Oman: Journalists Arrested for Criticizing Judiciary”. *Human Rights Watch*, August 5, 2016. https://perma.cc/FX3Y-6RBR.

———. 2016. “UAE: Free Two Jailed for Criticizing Egypt”. *Human Rights Watch*, May 15, 2016. https://perma.cc/JJX2-RNGR.

Hurwitz, Roger. 2014. “The Play of States: Norms and Security in Cyberspace”. *American Foreign Policy Interests*, 36(5): 322–331.

ictQatar. 2014. “Qatar National Cyber Security Strategy”. Government of Qatar, May 2014.

Ignatius, David. 2016. “The Cold War Is Over. The Cyber War Has Begun”. *Washington Post*, September 15, 2016. https://perma.cc/G2TK-NNAL.

Kaljurand, Marina. 2017. “An Interview with Marina Kaljurand, Former Minister of Foreign Affairs”. *Journal of Complex Operations*, December 21, 2017. https://perma.cc/K7F8-9MNX.

Khalid Negm. 2015. “Draft Law Concerning Electronic Crimes”. Leaked draft available on Scribd, April 2015. https://perma.cc/H4BS-VLGQ.

Lambert, Lisa, Anthony Deutsch, and Guy Faulconbridge. 2018. “West Accuses “pariah State” Russia of Global Hacking Campaign”. *Reuters*, October 5, 2018. https://perma.cc/YF3L-LV3N.

Malsin, Jared. 2018. “U.S. Releases $195 Million in Military Aid to Egypt”. *The Wall Street Journal*, July 25, 2018. https://perma.cc/Y7EY-F7UD.

Marczak, Bill, John Scott-Railton, Adam Senft, Ronald J. Deibert, and Bahr Abdul Razzak. 2018. “The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil”. Citizen Lab, October 1, 2018.

MCIT (Egypt). 2012. “National ICT Strategy 2012–2017: Towards a Digital Society and Knowledge-Based Economy”. MCIT, 2012.

———. 2014. “Publications—Egypt’s ICT Strategy 2014–2017”. Ministry of Communications and Information Technology. https://perma.cc/X6G3-WT3F.

MCIT (Saudi Arabia). 2011. “National Information Security Strategy”. Ministry of Communications and Information Technology, January 2011.

Miller, Elissa. 2018. “Egypt Leads the Pack in Internet Censorship Across the Middle East”. Atlantic Council, August 28, 2018. https://perma.cc/8DAC-LXYW.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. “Internet Security and Networked Governance in International Relations”. *International Studies Review* 15(1): 86–104.

National Cyber Security Center. 2017. “Profile—Introducing the National Cyber Security Center”. Govennnment of Saudi Arabia.

Rajab, Nabeel. 2016. “Letter From a Bahraini Jail”. *The New York Times*, September 4, 2016. https://perma.cc/HH4R-6WZP.

Raymond, Mark, and Laura DeNardis. 2015. “Multistakeholderism: Anatomy of an Inchoate Global Institution”. *International Theory*, 7(3): 572–616.

Reporters without Borders. 2014. “Cyber Crime Law Used Again to Silence Dissident Voices”. July 1, 2014. https://perma.cc/2M9U-S5E2.

———. 2016. “New Cyber Crimes Law Restricts Free Expression and Targets Online Activists”, January 21, 2016. https://perma.cc/M9ZB-6VRH.

Rij, Armida van, and Benedict Wilkinson. 2018. “Security Cooperation with Saudi Arabia: Is It Worth It for the UK?”. The Policy Institute at King’s, September 2018.

Saad, Ragab. 2015. “Egypt’s Draft Cybercrime Law Undermines Freedom of Expression”. Atlantic Council, April 24, 2015. https://perma.cc/9ATE-HNNA.

Salama, Samr. 2018. “Barlimani Yuʾakid ʾan Qanun Mukafihat Jaraʾim Al-Mu’alumat Al-Jadid Yauqif Al-Jaraʾim Al-ʾiliktroni [Parliament Confims That the New Law against Information Crimes Stops Electronic Crimes]”. *Al-Masry Al-Yaum*, August 19, 2018. https://perma.cc/D6HS-DFG4.

Savage, John E., and Bruce W. McConnell. 2015. “Exploring Multi-Stakeholder Internet Governance”. EastWest Institute, January 2015.

Segal, Adam. 2018. “Year in Review: Chinese Cyber Sovereignty in Action”. Council on Foreign Relations, January 8, 2018. https://perma.cc/L3UB-CDEN.

Staff Report. 2015. “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*, March 18, 2015. https://perma.cc/4QXP-Y8JR.

———. 2016. “Omani Jailed for Insulting UAE on Whatsapp”. *Al-ʿArabi Al-Jadid*, February 29, 2016. https://perma.cc/2ULR-LTFQ.

———. 2017. “CAIT Chief Briefs HH the Amir on National Cybersecurity Strategy—Vision to Protect Kuwait’s National Interest”. *Arab Times*, July 31, 2017. https://perma.cc/KTQ7-GW8G.

———. 2018a. “5-Year Jail, 3 Million Fine for Rumormongers”. *Saudi Gazette*, October 13, 2018. https://perma.cc/3D68-SFJC.

———. 2018b. “UAE Rights Activist Ahmed Mansoor Put on Trial in Abu Dhabi”. *Al-Jazeera*, April 18, 2018. https://perma.cc/8MWW-JCMV.

The Arab Republic of Egypt. 2014. “Egypt’s Constitution of 2014”. Constituteproject.org, translated by International IDEA.

The Economic Times. 2014. “China, Egypt Sign Strategic Partnership Agreement”, December 24, 2014. https://perma.cc/G5M4-KPHW.

UK Government. 2018. “UK Exposes Russian Cyber Attacks”, October 4, 2018. https://perma.cc/6UTX-TXYC.

UK Trade & Investment. 2013. “Cybersecurity: The UK’s Approach to Exports”. UK Government, April 2013.

Wikileaks. 2010. “US Embassy Kuwait City—Kuwait Interior Minister Sounds Alarm on Iran; Offers Assurances on GITMO Returnees and Security”. Wikileaks Public Library of US Diplomacy, February 17, 2010. Public Library of US Diplomacy. https://perma.cc/A79J-WF2E.

Yusif, Muhammad. 2016. “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*, May 11, 2016. https://perma.cc/KAX8-SUQH.

Zimmermann, Lisbeth. 2017. *Global Norms with a Local Face: Rule-of-Law Promotion and Norm Translation*. Cambridge, UK; New York: Cambridge University Press.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.