CYBERSECURITY IN THE MENA REGION: SHARED INSECURITIES, DIVERSE RESPONSES

ANALYSIS

JAMES SHIRES

25 MAY 2021

AL SHARQ
STRATEGIC
RESEARCH


DANGER

Contents

ABSTRACT	4
1. SHARED INSECURITIES	6
1.1 ACTOR-BASED SOURCES OF CYBER INSECURITY	7
1.2 STRUCTURAL SOURCES OF CYBER INSECURITY	9
2. DIVERSE RESPONSES	10
2.1 NATIONAL AND BILATERAL RESPONSES	11
2.2 REGIONAL AND INTERNATIONAL RESPONSES	13
CONCLUSION	15
ENDNOTES	17
ABOUT THE AUTHOR	20
AL SHARQ STRATEGIC RESEARCH	20

CYBERSECURITY IN THE MENA REGION: SHARED INSECURITIES, DIVERSE RESPONSES

Abstract: **Cyber insecurity is a multifaceted problem, and one further complicated by the political divides in the Middle East and North Africa (MENA). This paper tackles two questions: first, what are the main sources of cyber insecurity in the region? Second, how have states sought to respond to these cyber insecurities? The paper first highlights a range of cyber threat actors both inside and outside the region, as well as several structural factors that perpetuate cyber insecurities. The second part moves to state responses, treating national and international responses in turn. It argues that the MENA region demonstrates diverse responses to cyber insecurity. Nationally, states have sought to increase cybersecurity capacity, making significant institutional and bureaucratic changes to prioritize digital defense – and sometimes offense. Internationally, some states have participated in negotiations on international cyber norms, while others have remained apart. The paper concludes with several policy recommendations based on recent shifts in political alignment across the region.**

Cybersecurity is an uncomfortably elastic topic. It stretches from fundamental questions about privacy, identity, and freedom online, to the complex technological dependencies seemingly miraculously strung together to facilitate our daily digital lives. It encompasses new modes of economic activity, legal and illegal, as well as geopolitical issues around state competition and conflict. Cybersecurity issues are both global, in that they depend on transnational infrastructure and reshape geographical paradigms of international politics, and local, in that they appear differently in different contexts: social, national, and regional. Cybersecurity, including in Middle East and North Africa (MENA), is thus a multifaceted problem.[1] This paper provides a snapshot of cybersecurity in the MENA region, focusing on two questions: first, what are the main sources of cyber insecurity in the region? Second, how have states sought to respond to these cyber insecurities?

1- This paper takes the MENA region to include the Arabic-speaking states of northern Africa, the Arabian Peninsula, the Persian Gulf (including Iran), and the Levant (including Israel and the occupied Palestinian territories), with Turkey as the most north-easterly point. This definition follows standard practice but is, of course, slightly arbitrary.

These research questions deliberately move away from cybersecurity as a goal, ideal state, or best practice, to focus on cyber *insecurity*. One of the most immediately obvious aspects of cyber insecurity, in the MENA region and elsewhere, is the sheer range of threats: from the hacker stereotypes present in much popular culture to concerns around criminal gangs, spies, or soldiers acting in cyberspace. However, this focus on threat "actors" misses key sources of cyber insecurity that are not agential, but structural. Structural sources of cyber insecurity are aspects of digital economies and societies that enable threat actors to operate. These range from the socio-technical systems of vulnerability discovery, fixing, and updating that govern nearly all digital technologies, to the trust individuals and organizations must place in online interactions, especially during a global pandemic. This paper argues that key structural and agential sources of cyber insecurity are shared across the MENA region, providing a basis for common action.

The second research question focuses on states as a locus for responses to these sources of insecurity. This is not because states are the only actors who are able to muster sufficient responses. In many cases, state action is insufficient or even inappropriate for addressing such cyber insecurities without broader market-based cooperation or societal shifts. Nonetheless, states are key to cybersecurity responses, as experiences worldwide have shown that *laissez faire* approaches – whether in social media regulation against influence campaigns or encouraging companies to disclose and remedy data breaches - make little headway without state support or intervention. This paper argues that, despite shared insecurities in cyberspace, states in the MENA region have adopted noticeably diverse responses due to their varying political priorities. Some see strong, centralized institutional development as crucial to effective cybersecurity, while others have distributed both responsibility and capability across state organizations. Similarly, at an international level, some states have engaged extensively in cybersecurity governance negotiations, while others have remained apart, seeing distance from these processes as their best way to ensure flexibility and retain sovereignty.

This paper argues that, despite shared insecurities in cyberspace, states in the MENA region have adopted noticeably diverse responses due to their varying political priorities

The paper is structured around the two research questions. The first part analyzes sources of cyber insecurity in the MENA region, looking at agential and then structural factors. The second part moves to state responses, treating national and international responses in turn. The paper concludes with several policy recommendations based on recent shifts in political alignment across the region.

1. Shared insecurities

Understanding cyber insecurities as both a genuine digital threat and as perceived political precariousness is crucial for analyzing cybersecurity in the MENA region.[1] Cyber insecurities in the MENA region involve two kinds of insecurity, including the actor-based and structural distinctions above. The first kind of insecurities arises from intrusion or "hacking," defined as the ability to gain unauthorized access to digital devices and networks, and use that access for purposes contrary to the intent of their owners and designers.[2] These purposes can include exfiltration of data (in cases of political or industrial espionage and surveillance), altering or deleting data (such as "wiping" malware or ransomware, which encrypts target data until a ransom is paid for decryption), or even physical harm or destruction (where the targeted networks are industrial control systems or critical infrastructure).

The second kind of insecurity arises from the manipulation of digital networks, primarily social media platforms. There is now a broad consensus that social media platforms can be exploited for "influence campaigns", which promote political or other positions in illegitimate ways; for example, by using automated accounts (bots), by deliberately crafting verifiably false claims (disinformation), or by exploiting psychological vulnerabilities through microtargeted advertising. Both sets of insecurities can occur together, for example in "hack-and-leak" operations, where intrusion is used to obtain material that is then published for political advantage, or in "social engineering", where trust is used to gain access to a network without exploiting technical vulnerabilities.[3]

While these two sets of insecurities are both attributes of socio-technical systems, there is another, more political, sense of cyber insecurity underlying this discussion. Many states in the MENA region are authoritarian or hybrid systems, with façade democracies obscuring the political power of an entrenched elite or ruling figure. Such states are insecure not only in terms of intrusion or influence above, but also in terms of the position of the

incumbent regime. The series of popular protests known as the "Arab Spring" starkly demonstrated these insecurities, highlighting how social media can contribute (as one factor among many) to sweeping political changes and eventual outcomes as divergent as democratic transition, authoritarian retrenchment, or devastating civil war. While many states, including the Gulf countries and Egypt, realized the political potential of online political action after the Arab Spring, they did not associate these concerns with other cybersecurity issues until after the key incidents reviewed below - especially the 2012 "Shamoon" malware, which attacked the hard drives of Saudi Aramaco. Following Shamoon, the Gulf states invested extensively in cybersecurity expertise, both through high-profile commercial events and conferences and domestic education and awareness.[4]

1.1 Actor-based sources of cyber insecurity

Actor-based sources of cyber security in the MENA region can be classified in three main types: interstate competition and conflict, civil war contexts, and cybercrime. We will detail these three in turn. First, the MENA region is no exception to the states' worldwide adoption of cyber-espionage as a tool to advance their regional interests. Cybersecurity companies have attributed cyber-espionage campaigns targeting public and private entities to a number of Middle Eastern states, as well as notable cyber-espionage operations by global powers, such as the United States (US) and its allies, Russia, and China.[5] After the 2010 discovery of the infamous Stuxnet operation against Iran's nuclear program, disruptive state-attributed cyber operations have revolved around tensions in the Gulf, including Iranian wiping operations against critical infrastructure in Saudi Arabia since 2012 (including the "Shamoon" malware), US cyberattacks in response to Iranian provocations in 2019, and reported tit-for-tat exchanges between Israel and Iran in 2020.[6] The Gulf has also been the focus for state influence campaigns, as the Gulf crisis in 2017, was catalyzed by – and exacerbated – a highly divisive media environment, with government-supported social media manipulation especially directed against Qatar and Turkey.[7] The killing of Jamal Khashoggi in the Saudi consulate in Istanbul in 2018 was connected to private suppliers of targeted surveillance software, as well as influence campaigns on social media.[8]

Actor-based sources of cyber security in the MENA region can be classified in three main types: interstate competition and conflict, civil war contexts, and cybercrime

Aside from these inter-state disputes, similar activities have developed in civil war contexts. Cyber-espionage tools have been attributed to many actors in the Syrian civil war, most notably the regime-affiliated Syrian Electronic Army (SEA).[9] Members of the international coalition in Syria have claimed cyber operations against Islamic State, designed both to disrupt propaganda and to support kinetic action.[10] In Libya, disinformation is rife, with many parties to the conflict conducting social media propaganda, as well as social media campaigns emerging from media companies associated with external states such as Russia, Egypt and the UAE.[11] Some private military companies involved in the conflict have also been reported to offer cyberattack capabilities.[12] More generally, both civil wars and longstanding political disputes have provided sustained fuel for hacktivism in the region, as non-state actors have sought to raise the profile of various political issues – especially the Israel/Palestine conflict and Saudi-Iran tensions – through defacement and hack-and-leaks.[13]

Finally, a wide range of malicious actors use cyber tools for illicit financial gain. While these actors operate worldwide, there have been significant incidents by actors in the region, as well as ripple effects from worldwide campaigns.[14] In an early incident, there were two separate compromises of pre-paid credit card information of customers of Oman's Bank Muscat and the UAE's RAKBank in December 2012 and February 2013.[15] This information was provided to a transnational criminal network who withdrew $45 million in cash from ATMs across the world using the card details. In the years following, several strains of malware targeted mobile banking apps in the UAE.[16] More recently, two Iranians were indicted by the US for ransomware attacks against organizations worldwide, including hospitals.[17] Financial crime online also targets individuals and has significant gender-bias.[18] For example, blackmail following "sexting" or sharing of intimate pictures is an important but under-acknowledged aspect of cyber insecurity at a personal and family level, rather than that of the state.[19]

Both civil wars and longstanding political disputes have provided sustained fuel for hacktivism in the region, as non-state actors have sought to raise the profile of various political issues

1.2 Structural sources of cyber insecurity

We can also classify structural sources of cyber insecurity into three main types. The first is **geopolitical**, as the MENA region has been battered by the changing winds of US-China trade and technology competition. On the one hand, many MENA states have close relationships in security and defense with the US and its allies, including the Gulf states and NATO member Turkey. On the other hand, Chinese infrastructure investment, energy partnerships, and research in related technological fields of 5G and Artificial Intelligence (AI) are extremely attractive for these states. Therefore, they have sought to strike a balance between Chinese economic cooperation and US security requirements.[20] Geopolitical developments also affect MENA cyber insecurity in other ways. For example, the strengthening of EU data protection laws through the General Data Protection Regulation (GDPR) has led companies and individuals to demand similar privacy rights elsewhere, as well as mirroring data localization requirements and cloud computing regulation throughout the region, especially in the Gulf.[21] Finally, geopolitical divides manifest in physical form through the region's development of actual internet infrastructure. Rebuilding digital infrastructures after civil wars in Syria, Libya, and Yemen, as well as securing new city projects such as Neom in Saudi Arabia, adds a layer of complexity to the existing competition over - and continued exploitation of - cable laying and routing protocols in the region.[22]

A second structural source of cyber insecurity is **market-based**. There are significant difficulties in cybersecurity capacity-building in the MENA region that stem from the adverse incentives for the private sector – especially in critical infrastructure – to prioritize securing their digital networks over more short-term and reliable profits.[23] In addition, the cybersecurity industry is structurally dependent on vulnerability research

> ***This structural feature is exacerbated by the close links between many of these companies and military and intelligence agencies in their home states, meaning that the market for cyber tools blurs with and supports states' concurrent quest for their own capabilities***

for key security practices such as penetration testing. But these "white hat" security practices can also be used for "black hat" exploitation, and there are a growing number of companies doing such questionable research in MENA states, especially in Israel, Egypt, and the Gulf.[24] This structural feature is exacerbated by the close links between many of these companies and military and intelligence agencies in their home states, meaning that the market for cyber tools blurs with and supports states' concurrent quest for their own capabilities.

The third structural source of cyber insecurity lies in **the development of social media** in the MENA region. Almost all the big social media platforms originate from and are headquartered in the US, meaning that content moderation rules and broader "community standards" are crafted and applied for the US context or key markets such as Europe, and not the MENA region. States such as Saudi Arabia have resorted to unconventional methods to circumvent these constraints, such as recruiting insiders in Twitter's California offices to provide information on specific accounts.[25] More widely, most MENA states have relied on national-level surveillance architectures, supported by expansive cybercrime laws, to police social media for social and cultural norms, as well as suppress open political debate.[26] As with the exploit companies above, this has led – especially in the case of Egypt and Turkey – to negative publicity for companies providing such surveillance solutions.[27] Alternative social media platforms have been proposed by Saudi Arabia and the UAE, but with little success.[28]

2. Diverse responses

This section will further the discussion on the variety of state responses to the region's sources of cyber insecurity, whether agential or structural, by focusing first on MENA state actions at national and bilateral levels, and then on MENA contributions to international cybersecurity governance in international forums across the MENA region and more broadly. It should be stressed that state responses take many forms, including policy, legislative, and regulative initiatives. At a strategic level, we can also see state responses as seeking several distinct aims, including deterrence (dissuading threat actors from targeting that state), defense (improving cybersecurity protections and awareness, especially through capacity building), and resilience (ensuring the continuity of key state functions despite cyber disruption). In practice, state strategies and policies achieve these aims together, and so they are not sharply distinguished in the following discussion.

2.1 National and bilateral responses

According to the ITU Global Cybersecurity Index, conducted for the third time in 2018, Saudi Arabia, Oman, and Qatar were ranked the Arab world's top three countries in cybersecurity capacity, followed by Egypt, the UAE, Kuwait, and Bahrain.[29] These states have taken significant steps to securely digitalize government services, with the UAE ahead of the others in many respects, while other MENA states score more poorly. According to a 2019 study by Google and Bain & Company, the e-commerce market in 2017 in the MENA region overall was worth $8.3 billion and growing by 25% in pre-pandemic conditions.[30] This study, like other consultancies, sees Egypt and the Gulf states together as the cyber center of the MENA region, given that these states represent 80% of the MENA e-commerce market overall (excluding Israel). For cybersecurity specifically, according to market research consultancy Gartner, the value of cybersecurity sales doubled to just under $2 billion between 2014 and 2018.[31] Other companies offer more inflated figures, suggesting the Middle East cybersecurity market was worth $16 billion in 2020.[32]

A key element of cybersecurity capacity building is a national cybersecurity strategy. Most states, in the MENA region and worldwide, have published at least one such strategy, and many have updated their strategies several times.[33] Many MENA states have engaged in extensive cybersecurity education efforts, with universities offering undergraduate and graduate qualifications in technical and organizational aspects of cybersecurity, as well as more practical routes to professional cybersecurity roles and general awareness-raising. There has been significant adoption of these courses, especially by women, and the gendered aspects of cybersecurity professional and personal identities are powerful structuring factors for cybersecurity capacity, both in the MENA region and worldwide.[34]

Institutionally, some MENA states have centralized cybersecurity responsibilities in a single national cybersecurity organization. States who have taken this over the last

> ***In general, with the notable exception of Israel and Iran, MENA states are noticeable for their lack of public military cyber structures, not following the creation of separate "cyber commands" by many states worldwide***

year include Oman, Bahrain, and Qatar, while others have experimented with multiple institutional arrangements such as Egypt's Supreme Cybersecurity Council or the UAE's National Electronic Security Agency (NESA). Such organizations are designed to merge previously separate cybersecurity functions in communications and interior ministries, among others. The most sensitive aspect of this bureaucratic politics, for MENA states and counterparts in the US and Europe, is the relationship between such organizations and military and intelligence agencies. Scholars have shown how, in Turkey, this institutional competition has led to a dominant security role in such developments,[35] while others have critiqued the potential of such institutions in fractured, occupied, and contested spaces such as the Palestinian territories.[36] Other states, such as Tunisia, have sincerely pursued "multistakeholder" arrangements, involving public and private sectors as well as civil society representatives, in line with broader multistakeholder arrangements in global internet governance.[37] In general, with the notable exception of Israel and Iran, MENA states are noticeable for their *lack* of public military cyber structures, not following the creation of separate "cyber commands" by many states worldwide. This may be due to a lack of capability in general, or because the locus of cyber power lies elsewhere (in intelligence agencies, as noted above), or because these states prefer not to send potentially escalatory signals by establishing publicly offensive cyber programs.

Furthermore, states have pursued new or restrengthened bilateral partnerships that facilitate cybersecurity responses to a range of perceived threats, from vocal political opposition at home and abroad, to the potential consequences of cyber operations against critical infrastructure. The dynamics of such partnerships generally follow broader diplomatic alliances, although the GCC rift and the institutional inertia of the League of Arab States reveal the challenges of following established organizational lines. The paradigm example of a productive cybersecurity partnership is the one between the UAE and Saudi Arabia. Although not entirely in sync over Yemen and other flashpoints, their relationship has exemplified an agile, internationally embedded, public-private model for cybersecurity and information controls. Cybersecurity cooperation can also help to forge connections across longstanding fault lines. For example, the recent signing of the Abraham Accords, and Israel's normalization of relations with Bahrain, Sudan, UAE, and Morocco, means that Israel's strong cybersecurity sector can now openly export to the Gulf states, despite tensions with

democratic values.[38] The current thaw in relations between Egypt and Turkey may shift alliances in a different direction, however. Egypt has formerly relied on Saudi Arabia and the UAE to fund the purchase of expensive information controls,[39] although if this is a precursor to wider Turkish diplomatic engagement with the Gulf, then cybersecurity cooperation might well be a useful diplomatic card for all sides.

Part of the reason for the shifting alignments above, especially the Israeli moves, is to counter Iran's success in a very different mode of cybersecurity cooperation. In contrast to the states above, Iran has deliberately increased its technical isolation from the internet infrastructure of other MENA states, using the temporary shutdowns following fuel-price protests in 2019 to adjust its domestic internet architecture towards more centralized control. At the same time, Iran has also cultivated a significant "hacker" scene, with talented individuals sometimes going on to work for companies tasked by the Iranian military and intelligence, or even working within these organizations themselves.[40] While this may be an efficient solution given limited Iranian resources, the restrictions on such individuals have led to the exposure of key capabilities and reported conflicts within such groups.[41] Iran has also reportedly worked on digital intelligence gathering with proxies in various conflict zones, likely deploying malware in the Syrian conflict.[42] Finally, Israeli kinetic strikes against Hamas cyber teams indicate a confluence between offline and online struggles between the two adversaries across Syria and Lebanon.[43]

2.2 Regional and international responses

This section moves from the national and bilateral responses above to consider cybersecurity developments connecting the MENA region to other regions and international processes. First, there are several transnational cybersecurity capacity

> ***This early idea came to fruition much later, in March 2020, with the launch of the Internet Infrastructure Security Guidelines for Arab States by the Internet Society, a transnational non-profit organization with both state and corporate members***

building initiatives with a MENA focus.[44] One of the earliest attempts was a proposal for a "pan-Arab observatory" in 2009, based in Lebanon, that would elect members from all Arab states. The proposal included several Lebanese ministries (interior and justice), as well as information technology (IT) associations and universities in Lebanon and the League of Arab States. This early idea came to fruition much later, in March 2020, with the launch of the Internet Infrastructure Security Guidelines for Arab States by the Internet Society, a transnational non-profit organization with both state and corporate members.[45] This initiative – including a new observatory - demonstrates that multistakeholder processes remain useful in the MENA region, as it offers practical steps for organizations to secure routing mechanisms and improve cybersecurity practices. More generally, MENA states have participated across international cybersecurity governance processes, including a Group of Governmental Experts (GGE) and Open Ended Working Group (OEWG) in the UN. Iran, despite disassociating itself from the consensus final report of the OEWG, agreed in March 2021.

These broader international processes are separate from extensive international negotiations over cybercrime. The main international legal text on cybercrime is the Budapest Convention on Cybercrime, agreed by the Council of Europe in 2001. Following the Budapest Convention, which has 65 ratifications or signatures/accessions and only four in the MENA region (Turkey, Israel, Morocco, and Tunisia), the League of Arab States introduced a Convention on Combating Information Technology Offences. Originally conceived in 2004 as a pan-Arab "model law" for combating information technology offences, the Arab Convention was finally signed in December 2010. The Arab Convention, and the simultaneous events of the Arab Spring, led to the development of controversial cybercrime laws throughout the region, criticized by many as including ambiguous clauses used for repression.[46] Current international negotiations in the UN are revisiting the idea of a global cybercrime treaty, with a 2019 resolution proposed by Russia swiftly approved by nearly all MENA states, but the impact of these negotiations on domestic legislation will not appear for several years, if at all.

Compared to cybercrime, an equally tricky area of negotiation is in the applicability of international laws of armed conflict to cyber operations, and the more specific implementation of norms on responsible state behavior in cyberspace, agreed at the GGE in 2015 and subsequently across several multistakeholder processes, albeit with limited representation from the region. Such norms include the protection of critical infrastructure, clearly violated

by some of the state operations listed in previous sections, as well as protection of the internet's "public core."[47] Other related initiatives, such as confidence-building measures (CBMs) to reduce the risk of escalation for cyber operations, are only beginning to gain ground in the MENA region. More practically, the inclusion of technical bodies, such as national Computer Emergency Response Teams (CERTs), in international information sharing and dialogue mechanisms, serves to *de facto* provide channels of communication that may be useful in crisis scenarios.[48]

Conclusion

To conclude, I first offer four broad policy recommendations based on the above discussion and other recent work,[49] and then end by reflecting on the double sense of insecurity with which the paper began.

- First, government, private sector, and civil society organizations should work together to increase cyber resilience. Together, they need to identify the relative strengths and weaknesses of each stakeholder, seeking to compensate for these weaknesses through diverse strengths.

- Second, states should develop education and training as a core basis for national and regional cybersecurity. Educational initiatives should be coordinated across the region and should prioritize gender and intersectional equality.

- Third, states should invest in credibility and long-term reliability in cybersecurity action and communication. This means crafting cybersecurity policy and regulation that is accessible, clear in both substance and scope of application, and consistently interpreted and enforced.

- Fourth, states should work internationally to raise the level of cybersecurity in the region. States can use concepts of responsible state behavior and the "public core" of the internet as a basis to invest in broader international cybersecurity governance processes, developing international law and participating in relevant working groups at the UN.

Finally, this paper has underlined the dual sense of cyber insecurity prevalent in the MENA region. Cyber insecurities, both actor-based and structural, present clear risks to core state functions: the stability of digital economies, the smooth functioning of national and transnational critical infrastructures, and the protection of vulnerable individuals online and offline. But cyber insecurities are also incorporated into broader political insecurities, especially in states and regions where incumbent rulers are involved in internationalized civil wars, or stifle dissenting voices to prevent popular protest. In this way, cyber insecurities - both intrusion into digital networks and the manipulation of social media platforms – represent threats to domestic and regional political power, as well as to the state functions above. Consequently, states have invested in cybersecurity responses not only with a view to improve cybersecurity for individuals and commercial organizations in the region, but more fundamentally to preserve elites' position and status, while diminishing or destabilizing that of their adversaries. As the MENA region becomes ever more digital, with young and fast-growing populations pushing the percentage of individuals online ever higher, cyber insecurities will not only translate into political insecurity, but will increasingly be the central medium of political participation and contest over its future.

Endnotes

1- Bassant Hassib and James Shires, "Manipulating Uncertainty: Cybersecurity Politics in Egypt," *Journal of Cybersecurity* 7, no. 1 (2021).

2- James Shires, "Family Resemblance or Family Argument? Three Perspectives of Cybersecurity and Their Interaction," *St Anthony's International Review* 14, no. 3 (2019): 18–36.

3- James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy* 4, no. 2 (2019): 235–56; James Shires, "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics," *Texas National Security Review*, August 2020.

4- James Shires, "Enacting Expertise: Ritual and Risk in Cybersecurity," *Politics and Governance* 6, no. 2 (2018): 31–40.

5- McAfee Labs, "Global Energy Cyberattacks: 'Night Dragon'" (McAfee, February 10, 2011); Symantec Security Response, "Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance v1.1" (Symantec, August 27, 2015); Kaspersky Lab, "The Desert Falcons Targeted Attacks," Securelist - GREAT, February 17, 2015, https://perma.cc/BE9U-3NG5; GReAT, "The Mystery of Duqu 2.0: A Sophisticated Cyberespionage Actor Returns," Securelist - GREAT (Kaspersky Lab), https://perma.cc/EVW3-XS4Q.

6- Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (May 1, 2013): 81–96; Kaspersky Lab, "From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond" (Kaspersky Lab Global Research and Analysis Team, March 7, 2017); J.D. Work and Richard J. Harknett, "Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges," Issue Brief (Washington, D.C: Atlantic Council, July 2020).

7- James Shires, "The Cyber Operation against Qatar News Agency," in *The 2017 Gulf Crisis: An Interdisciplinary Approach*, ed. Mahjoob Zweiri, M. Mizanur Rahman, and A. Kamal (Berlin Heidelberg: Springer Nature, 2020); James Shires, "Disinformation in the Gulf," in *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, ed. Michael Sexton and Eliza Campbell (Middle East Institute, 2020), 93–107.

8- Bill Marczak et al., "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil" (Citizen Lab, October 1, 2018); Craig Timberg and Sarah Dadouch, "When U.S. Blamed Saudi Crown Prince for Role in Khashoggi Killing, Fake Twitter Accounts Went to War," *Washington Post*, March 2, 2021, https://www.washingtonpost.com/technology/2021/03/02/saudi-khashoggi-twitter-mbs/.

9- Ahmed K. Al-Rawi, "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army," *Public Relations Review* 40, no. 3 (September 1, 2014): 420–28, https://doi.org/10.1016/j.pubrev.2014.04.005; Marie Baezner, "The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict," CSS Cyber Defense Project (Center for Security Studies: ETH Zurich, October 18, 2017).

10- Mike Burgess, "Director-General ASD Speech to the Lowy Institute," Australian Signals Directorate (ASD), March 27, 2019, https://perma.cc/VVM3-GZHX; Michael Martelle and Audrey Alexander, "Operation Glowing Symphony: The Missing Piece in the US Online Counter-ISIS Campaign," in *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, ed. Michael Sexton and Eliza Campbell (Middle East Institute, 2020), 108.

11- DFRLab, "Facebook Disabled Assets Linked to Egypt and UAE-Based Firms," Medium, August 14, 2019, https://medium.com/dfrlab/facebook-disabled-assets-linked-to-egypt-and-uae-based-firms-a232d9effc32; Shelby Grossman, Khadija H., and Renee DiResta, "Blurring the Lines of Media Authenticity: Prigozhin-Linked Group Funding Libyan Broadcast Media," The Stanford Internet Observatory Cyber Policy Center, March 20, 2020, https://cyber.fsi.stanford.edu/io/news/libya-prigozhin.

12- Samer Al-Atrush and David Wainer, "Western Team Went to Help Moscow's Man in Libya, UN Finds," *Bloomberg*, May 14, 2020, https://perma.cc/CE7Q-FRSC.

13- Adrian Chen, "A Chat With the Teen Saudi Hacker Who Says He Stole a Million Israeli Credit Cards," Gawker, January 6, 2012, https://perma.cc/9WT9-7LCH; Carl Nasman, "Anonymous Hacktivist Explains Why

Group Is Targeting Saudi Arabian Government," DW.COM, October 2, 2015, https://perma.cc/WQ3Z-FZX6; Shahin Azimi, "Iran-Saudi Tensions Erupt in 'Cyberwar,'" *BBC News*, June 3, 2016, https://perma.cc/8PH3-Z6LY.

14- Naushad Cherrayil, "UAE Is Second Most Targeted Country in Middle East and Africa for Ransomware," Gulf News, May 2, 2017, https://perma.cc/7ML3-N7DB.

15- Brian Krebs, "Crooks Net Millions in Coordinated ATM Heists," *Krebs on Security* (blog), February 2013, https://perma.cc/9MSZ-QJ8F.

16- Kevin Sun, "BankBot Seen on Google Play, Targets New UAE Bank Apps," Trend Micro, September 13, 2017, https://perma.cc/4YDK-BXC5.

17- Department of Justice, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Office of Public Affairs, November 28, 2018, https://perma.cc/JA9E-P34N.

18- Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security" (Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020); Katharine M. Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response" (Geneva: UN Institute for Disarmament Research (UNIDIR), January 2021).

19- BBC, "Sex, Honour, Shame and Blackmail in an Online World," *BBC News*, October 26, 2016, sec. Magazine, https://perma.cc/Y3JT-6FY8.

20- James Shires and Joyce Hakmeh, "Is the GCC Cyber Resilient?" (London: Chatham House Royal Institute for International Affairs, March 2020).

21- Rouda Alamir Ali, "Cloud Computing in Arab States: Legal Aspect, Facts and Horizons" (ITU Arab Regional Office, July 2016); Robert Mogielnicki, "Sovereign Data: The Development and Marketing of Bahrain's Digital Domain," in *The Hague Program for Cyber Norms* (Moving forward, Leiden University, 2020).

22- Loqman Salamatian et al., "The Geopolitics behind the Routes Data Travels: A Case Study of Iran," *ArXiv:1911.07723 [Cs]*, November 19, 2019, http://arxiv.org/abs/1911.07723; Rory Jones and Drew Fitzgerald, "Google Plans Fiber-Optic Network to Connect Via Saudi Arabia and Israel for First Time," *Wall Street Journal*, November 23, 2020, https://perma.cc/NK6C-LRFD.we need to comprehend Cyberspace as a space organized by humans to analyse the strategies of the actors. This geography requires a multidisciplinary dialogue associating geopolitics, computer science and mathematics. Cyberspace is represented as three superposed and interacting layers: the physical, logical, and informational layers. This paper focuses on the logical layer through an analysis of the structure of connectivity and the Border Gateway Protocol (BGP

23- Shires and Hakmeh, "Is the GCC Cyber Resilient?"

24- Winnona DeSombre et al., "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service" (Washington, D.C: Atlantic Council Cyber Statecraft Initiative, February 2021).

25- Alex Kantrowitz, "How Saudi Arabia Infiltrated Twitter," BuzzFeed News, February 19, 2020, https://www.buzzfeednews.com/article/alexkantrowitz/how-saudi-arabia-infiltrated-twitter.

26- James Shires, "Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf," in *Governing Cyberspace: Power, Behavior, and Diplomacy*, ed. Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield Publishers, Inc., 2020), 205–26.

27- Bill Marczak et al., "Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?" (Citizen Lab, March 9, 2018).

28- Bill Marczak, "How Abu Dhabi's Spy Sheikh Hid ToTok in Plain Sight," Medium, January 2, 2020, https://perma.cc/KG62-SMWU; Staff Report, "Al-Badeel al-Sa'udi Li"Whatsapp".. Kulu Ma Turidu Ma'rifatahu 'an Tatbiq 'Pingme' [The Saudi Alternative to Whatsapp... All You Want to Know about the the Pingme App]," El-Nabaa, January 18, 2021, https://perma.cc/AWE9-VJ6M.

29- ITU, "Global Cybersecurity Index (GCI) 2018" (ITU Publications, 2018).
30- Bain&Company and Google, "E-Commerce in MENA: Opportunity beyond the Hype," 2019; Robert Mogielnicki, "Add to Cart: E-Commerce Development in the Gulf," *Arab Gulf States Institute in Washington* (blog), December 18, 2019, https://agsiw.org/add-to-cart-e-commerce-development-in-the-gulf/.
31- Gartner, "Gartner Says Middle East & North Africa Information Security Spending to Reach US$1.3 Billion in 2016," October 31, 2016, https://perma.cc/3LWW-GUGP; Sony Shetty, "Gartner Says Middle East and North Africa Enterprise Information Security Spending Will Grow 9.8 Percent in 2019," Gartner, October 22, 2018, https://perma.cc/9H6R-C38E.
32- MarketsandMarkets, "Middle East Cybersecurity Market Worth $29.9 Billion by 2025," PRNewswire, June 16, 2020, https://perma.cc/27Z3-YH5Y.
33- James Shires, *The Politics of Cybersecurity in the Middle East* (London, UK: Hurst, forthcoming).
34- Millar, Shires, and Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response."
35- H. Akin Unver, "The Logic of Secrecy: Digital Surveillance in Turkey and Russia," *Turkish Policy Quarterly* 17, no. 2 (September 28, 2018), http://turkishpolicy.com/article/923/the-logic-of-secrecy-digital-surveillance-in-turkey-and-russia.
36- Fabio Cristiano, "Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative," *Cyber Orient* 13, no. 1 (2019): 28–42; Tuba Eldem, "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security," *International Journal of Public Administration* 43, no. 5 (April 3, 2020): 452–65, https://doi.org/10.1080/01900692.2019.1680689.
37- Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7, no. 3 (November 2015): 572–616.
38- Elham Fakro, "What the Abraham Accords Reveal About the United Arab Emirates," War on the Rocks, October 30, 2020, http://warontherocks.com/2020/10/what-the-abraham-accords-reveal-about-the-united-arab-emirates/.
39- Bassant Hassib and Nardine Alnemr, "Securitizing Cyber Space in Egypt: The Dilemma of Cybersecurity and Democracy," in *Routledge Companion to Global Cyber-Security Strategy*, ed. Scott N. Romaniuk and Mary Manjikian (Routledge, 2020).
40- Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press, 2018); Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge" (Carnegie Endowment for International Peace, 2018).
41- Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed" (Recorded Future Insikt Group, May 9, 2018); Catalin Cimpanu, "New Leaks of Iranian Cyber-Espionage Operations Hit Telegram and the Dark Web," ZDNet, May 9, 2019, https://perma.cc/MRN6-QUFC.
42- John Scott-Railton et al., "Group5: Syria and the Iranian Connection" (Citizen Lab, August 2, 2016).
43- Robert Chesney, "Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility," Lawfare, May 6, 2019, https://perma.cc/5X56-4JMR.
44- Nir Kshetri, "Cybersecurity in the Gulf Cooperation Council Economies," in *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (New York, NY: Springer, 2016), 183–94.
45- Internet Society, "Internet Infrastructure Security Guidelines for the Arab States," March 2020.
46- Shires, "Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf."
47- Dennis Broeders and Bibi Van den Berg, *Governing Cyberspace: Behavior, Power and Diplomacy*, Illustrated Edition (Lanham: Rowman & Littlefield, 2020).
48- Leonie Maria Tanczer, Irina Brass, and Madeline Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy," *Global Policy* 9, no. S3 (2018): 60–66, https://doi.org/10.1111/1758-5899.12625.
49- These recommendations also draw from discussions at a workshop on Cyber Resilience in the GCC, held by Chatham House virtually on 30 March 2021.

ABOUT THE AUTHOR

James Shires is an Assistant Professor in Cybersecurity Governance at the Institute for Security and Global Affairs, University of Leiden, a fellow with the Cyber Statecraft Initiative at the Atlantic Council, and an Associate Fellow with The Hague Program for Cyber Norms. He has written extensively on cybersecurity and international politics and is the author of "The Politics of Cybersecurity in the Middle East" (Hurst/Oxford University Press, 2021).

AL SHARQ STRATEGIC RESEARCH

A think tank that looks to undertake impartial, rigorous research to promote the ideals of democratic participation, an informed citizenry, multi-stakeholder dialogue and social justice.

Address: Istanbul Vizyon Park A1 Plaza Floor:6
No:68 Postal Code: 34197
Bahçelievler/ Istanbul / Turkey
Telephone: +902126031815
Fax: +902126031665
Email: info@sharqforum.org

AL SHARQ STRATEGIC RESEARCH
للأبحاث الاستراتيجية

research.sharqforum.org

SharqStrategic