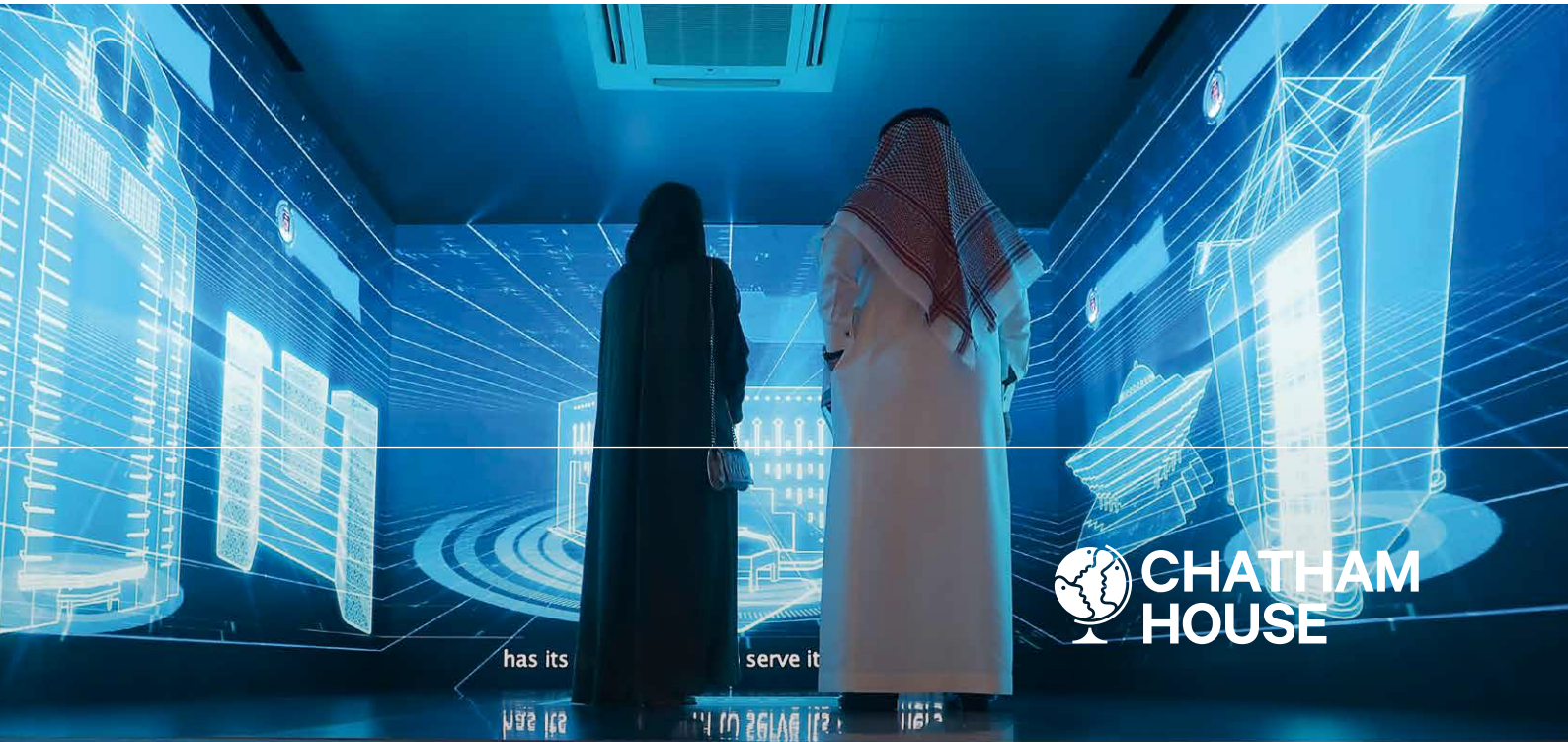
Briefing
March 2020
International Security
Programme

Is the GCC Cyber Resilient?

James Shires and Joyce Hakmeh

Summary

- GCC states seek to be leaders in digital innovation, but this leaves them vulnerable to an increasing range of cyberthreats. Governments have invested significantly in cybersecurity but these measures have been unevenly implemented, making it difficult for these states to be resilient against a large-scale cyber incident.
- Strategies, structures and processes ('approaches') for achieving cyber resilience can be conceptualized along a scale from *centralized* to *distributed*: centralized approaches maintain decision-making power in a single body, while distributed ones disperse power over many sites.
- Centralized approaches provide more resilience against unwanted influence, while distributed approaches provide more resilience against intrusions into infrastructure. The GCC states have so far prioritized centralized over distributed cyber resilience, seeking internet and social media control over sustainable network recovery.
- GCC governments should make a sustainable commitment to cyber resilience that provides clear guidance to organizations and makes best use of emerging cybersecurity structures. This may involve further engagement with international initiatives and partners to increase cyber resilience.
- Given limited resources, GCC governments should rebalance their efforts from centralized towards distributed approaches to resilience.
- GCC governments should examine the impact of relevant new technologies, discussing openly the risks of these technologies and appropriate solutions.



Introduction

How would the states of the Gulf Cooperation Council (GCC) respond to a serious cyber incident? This could be a global ransomware event, a critical infrastructure incident targeted at the energy sector, or a significant denial of service attack on key government departments. Alternatively, it could be the manipulation of public opinion from within the region or without. These cyber incidents could occur together, involving leaked information gained through hacking and publicized through social media. The high likelihood of such events means that cyber resilience (the ability to withstand and rapidly recover from disruption) is at least as important as cybersecurity (protection against those threats). This paper examines cyber resilience in the states of the GCC: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE). The national cybersecurity strategies of these states explicitly link cybersecurity with the concept of resilience (in Arabic: *murūna*), for example in ensuring the continuity of IT systems (Dubai), the functioning of infrastructure (Bahrain), and preserving wider social and cultural aspects of cyberspace (Qatar, Saudi Arabia).[1] Given these aims, this paper seeks to support GCC states in their efforts to improve cyber resilience in a sustainable and coherent manner.

Recently, the landscape of cyberthreats has expanded from issues like denial of service, malware and digital sabotage to include online influence operations, highlighting vulnerabilities in social as well as technological information systems.[2] In the GCC, threats to information security have been the focus of cybersecurity efforts since the 2011 'Arab Spring', which governments perceived as a demonstration of the new social dangers stemming from digital communications technologies.[3] Information threats have attracted renewed attention due to internal divisions within the GCC following the Qatar split in 2017. This paper employs a broad approach to cyber resilience, taking into account both resilience to 'traditional' cyberattacks and strategic control of the information environment.

This paper conceptualizes approaches to cyber resilience along a scale from *centralized* to *distributed*: centralized approaches to resilience maintain decision-making power and processes in a single location or body, while distributed approaches disperse power and processes over many sites. As suggested in the following section, the former is more able to counter strategic information threats, while the latter is better suited to countering more frequent but disparate intrusions into networks. Research for this paper shows that cybersecurity measures in the GCC are overly centralized, designed to control the information environment rather than recover from damaging cyberattacks. Consequently, this paper argues that these countries should take a balanced approach to cyber resilience that recognizes limited cybersecurity resources and includes international engagement with other states, multinational companies and international organizations, as well as an early government appraisal of the opportunities and risks presented by new technologies.

---

[1] Dubai Electronic Security Center (2017), *Dubai Cyber Security Strategy*, Government of Dubai, p. 19, https://desc.dubai.ae/res/wp-content/uploads/DCSS-EN.pdf; eGovernment Portal (2017), *Kingdom of Bahrain – EGovernment Portal Cybersecurity Strategy*, Government of Bahrain, 3 October 2017, https://perma.cc/RSL4-FPJA (ENG), https://perma.cc/NNP2-CGBJ (AR); ictQatar (2014), *Qatar National Cyber Security Strategy*, Government of Qatar, p. 1, https://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf (accessed 21 Feb. 2020); National Cyber Security Center (2017), *Profile – Introducing the National Cyber Security Center,* Government of Saudi Arabia, p. 5.

[2] For some states, information threats have always been their major concern, see below.

[3] This is only one among many effects of the January 2011 revolutions on the GCC, and the complex origin of the protests themselves cannot be attributed only to new communications technologies.

The methodology of this study is inductive and qualitative, drawing on a range of evidence in relation to different areas of cyber resilience, including laws, regulations, strategies and policies, and limited available data about the cybersecurity practices of GCC governments and private organizations in the region. The paper focusses on overall trends and uses individual case studies to illustrate these trends rather than individually examining each GCC state. The aim is to stay at a high level of analysis across the GCC, dipping into empirical detail briefly while taking into account internal differences. This paper follows two earlier research papers in this series on cybersecurity in the GCC: the first on the digital economy, and the second on cybercrime legislation and human rights.[4]

The paper is structured in five sections. The first section provides the theoretical basis for the analysis, introducing the distinction between centralized and distributed approaches to cyber resilience. The second section outlines the double threat perception of the GCC states, including both information-based and 'traditional' cyberthreats. The third section provides an overall picture of cyber resilience in the GCC, while the fourth examines the relationship between centralized and distributed approaches to cyber resilience in the region. The fifth and final section examines new technologies and their implications for cyber resilience in the GCC.

Distributed and centralized cyber resilience

Security seeks to avoid and respond to failure and disruption, while resilience aims to sustain holistic function and increase capacity for its continuation in any eventuality

Resilience is, according to a US Presidential Policy Directive issued in 2011, 'the ability to adapt to changing conditions and withstand and rapidly recover from disruption'.[5] The most precise statement of resilience in GCC national cybersecurity strategies follows this definition closely, stating that resilience is 'the ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents'.[6] Resilience and security have subtly different objectives: security seeks to avoid and respond to failure and disruption, while resilience aims to sustain holistic function and increase capacity for its continuation in any eventuality.[7] There are nonetheless many overlaps between cybersecurity and cyber resilience, both conceptually and in terms of relevant practices. This paper draws on many indicators of cybersecurity and cyber risk. The concept of resilience can be applied at many levels, from individual organisms to whole societies and ecosystems.[8]

Resilience is an important property of information and communications systems. In the early twentieth century, the field of cybernetics sought to create resilient systems that would self-adjust based on environmental feedback.[9] A more direct

[4] Hakmeh, J. (2017), *Cybercrime and the Digital Economy in the GCC Countries,* Research Paper, London: Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf; Hakmeh, J. (2018), *Cybercrime Legislation in the GCC Countries: Fit for Purpose?,* Research Paper, London: Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf.

[5] Obama, B. (2011), *Presidential Policy Directive PPD/8 Subject: National Preparedness*, The White House, 30 March 2011, p. 6. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness (accessed 21 Feb. 2020).

[6] ictQatar (2014), *Qatar National Cyber Security Strategy*, p. 24.

[7] For a deeper philosophical derivation and discussion, see Zebrowski, C. (2013), 'The Nature of Resilience', *Resilience* 1(3): pp. 159–73, https://doi.org/10.1080/21693293.2013.804672; Brassett, J., Croft, S. and Vaughan-Williams, N. (2011), 'Special Issue: Security and the Politics of Resilience', *Politics* 33(4); Dunn Cavelty, M., Kaufmann, M. and Kristensen, K. (2015), 'Special Issue: Resilience and (in)security): practices, subjects, temporalities', *Security Dialogue,* 46(1).

[8] For a critique of the relationship between resilience at a societal and individual level see Evans, B. and Reid, J. (2014), *Resilient Life: The Art of Living Dangerously*, Cambridge: Polity.

[9] Wiener, W. (1965), *Cybernetics, or the Control and Communication in the Animal and the Machine,* Cambridge, Mass: The MIT Press.

lineage of resilience comes from packet-switching, proposed in the 1960s as a way for US military communications to be more resilient in the event of a Soviet nuclear strike, and then incorporated into the Internet Protocol (IP) as the standard for the US Department of Defence's ARPANET in the 1970s.[10] Two of the three core concepts of information security – integrity and availability – are directly related to resilience, ensuring that information flows remain trusted and continuous despite attacks.[11] Cyber resilience, then, is at base the resilience of digital information systems.[12]

Cyber resilience, however, does not apply to information systems only in the narrow terms above, describing digital networks of hardware and software. As Schneier and Farrell argue in their analysis of US election interference, whole states can be modelled as information systems, drawing on a wider scholarship of globalization and information flows.[13] Cyber resilience, in this view, also includes the broader ability of states to withstand strategic influence operations aimed at disrupting or manipulating information flows between citizens, politicians and other domestic actors. A comprehensive approach to cyber resilience includes both resilience to 'traditional' cyberattacks and to strategic attempts to influence the information environment of a state.[14]

Like security, resilience is relative to threat.[15] A system that is resilient to one set of threats may not be resilient to others, and, more problematically, steps taken to increase resilience in some ways may decrease resilience in others.[16] It is therefore necessary to consider the resilience of different types of systems. Specifically, the paper identifies centralized systems, in which a single node entirely controls the processes of other nodes, and distributed systems, in which tasks are completed asynchronously, independently and concurrently.[17] This is a spectrum rather than a binary division, with decentralization a mid-point between the two.[18]

[10] Baran, P. (1964), 'Memorandum RM-3420-PR On Distributed Communications: 1. Introduction to Distributed Communications Networks', United States Air Force Project Rand, https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf (accessed 21 Feb. 2020); Leiner, B., Cerf, V., Clark, D., Kahn, R. and Kleinrock, L. (1997), 'A Brief History of the Internet', *ACM SIGCOMM Computer Communication Review*, 39(5): pp. 22–31.

[11] Although confidentiality often occupies prime position in cybersecurity discussions, cyberattacks targeting integrity and availability, such as denial of service and ransomware, have recently been at the forefront of international policy discussions (e.g. Mirai, Wannacry).

[12] See Herrington, L. and Aldrich, R. (2013), 'The Future of Cyber-Resilience in an Age of Global Complexity', *Politics* 33(4): pp. 299–310, https://doi.org/10.1111/1467-9256.12035. Their discussion highlights that distributed approaches to cyber resilience are not necessarily planned, with extensive 'systems diversity' in the UK due to the presence of legacy infrastructure.

[13] Schneier, B. and Farrell, H. (2018), *Common-Knowledge Attacks on Democracy,* Berkman Klein Center for Internet and Society: Harvard University. We recognize that the information environment of a state, especially in the digital era, is not easily distinguishable from that of a region or the whole world. However, the 'territorializing practices' of states in applying national geographic borders to cyberspace mean that this is increasingly becoming a viable way of thinking about information flows. In other words, 'of' is not identical to the conceptually problematic 'within' a state. See Lambach, D. (2019), 'The Territorialization of Cyberspace', *International Studies Review*, viz022, https://doi.org/10.1093/isr/viz022.

[14] A good example of a narrower approach, focusing only on network security, is Bissell, K., Lasalle, R., Dool, F. van den and Kennedy-White, J. (2018), *Gaining Ground on the Attacker: 2018 State of Cyber Resilience,* Accenture Security.

[15] Cavelty, M. D., Kaufmann, M. and Kristensen, K. S. (2015), 'Resilience and (in)Security: Practices, Subjects, Temporalities', *Security Dialogue,* 46(1): pp. 3–14, https://doi.org/10.1177/0967010614559637.

[16] Ross, R., McEvilley, M. and Oren, J. (2018), *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-160v1.

[17] This is an extreme simplification of a large and complex field. For an introduction, see Maier, M. W. and Rechtin, E. (2009), *The Art of Systems Architecting*, 3rd edition, Boca Raton: CRC Press.

[18] Hierarchies are possible even in distributed systems, although they depend on group nominations in both social and technical versions.

Distributed systems are widely thought to be more resilient than centralized systems, largely because they do not have a single point of failure.[19] However, for some threats and tasks, distribution can be less resilient than centralization.[20] In particular, strategic threats requiring coordinated responses as a whole may be better countered in a centralized system, while lower-level threats impacting part of a system would be better countered in a distributed system.[21] For example, the definition of cyberthreats to the US has expanded following Russian influence operations in the 2016 US presidential election, and disparate private-sector responses have been replaced by calls for a 'whole-of-nation' response: in short, moving from a distributed to a centralized approach to cyber resilience.[22]

This shift in the US demonstrates that the distinction between distributed and centralized systems is not exactly equivalent to that between democratic and authoritarian political systems.[23] Recent scholarship on information operations in the US focuses on 'democracy's dilemma': the idea that improving democratic resilience to foreign influence operations could damage the practice of democracy itself.[24] This dilemma is drawn from parallels to Samuel Huntingdon's 'King's Dilemma', in which autocratic leaders face a choice between stability and modernization. The King's Dilemma has been applied often to the autocratic monarchal systems of the GCC states.[25] In contrast, the distributed/centralized distinction allows us to move away from distinctive democratic/autocratic dilemmas towards a cyber resilience framework that can be applied across states, while avoiding what Schneier and Farrell call an 'easy equivalence' between democracies and autocracies.[26]

The GCC view of cyberthreats

All GCC countries face significant 'traditional' threats in cyberspace, including ransomware, cybercriminal fraud, and hacktivism.[27] These threats have targeted individuals, commercial organizations and state entities.[28] More specifically, the GCC has been the target of many advanced persistent threats (APTs) or state-sponsored campaigns. State-sponsored threats come in several guises: for example, global energy sector cyberespionage has been traced to China and Russia, while the Snowden

[19] Matni, N., Leong, Y., Wang, Y., You, S., Horowitz., M. and Doyle, J. (2014), 'Resilience in Large Scale Distributed Systems', *Procedia Computer Science*, Conference on Systems Engineering Research, 28, pp. 285–93, https://doi.org/10.1016/j.procs.2014.03.036.
[20] Goldman, H. (2010), *Building Secure, Resilient Architectures for Cyber Mission Assurance*, The MITRE Corporation.
[21] It is worth noting that cyber and other threats can also be characterized as distributed or centralized: for more details, see US Department of Homeland Security and US Department of Commerce (2018), *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats,* 22 May 2018, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=925900 (accessed 21 Feb. 2020).
[22] Rosenbach, E. and Mansted, K. (2018), *Can Democracy Survive in the Information Age?*, Belfer Center for Science and International Affairs, Harvard Kennedy School. We use 'approach' as a looser term than 'system' to refer to strategies, structures and processes in this paper.
[23] Although the terminology of systems architecture, with 'master-slave' and 'peer-to-peer' relationships describing centralized and distributed systems, respectively, deliberately reflects certain social relationships.
[24] Farrell, H. and Schneier, B. (2019), 'Democracy's Dilemma', *Boston Review*, https://perma.cc/JW5F-EEFF.
[25] For example, Kostiner, J. (2000) (ed.), *Middle East Monarchies: The Challenge of Modernity*, Boulder, Colo: Lynne Rienner Publishers.
[26] Farrell, H. and Schneier, B. (2019), 'Democracy's Dilemma'. Our analysis highlights what Ennis terms the 'entrepreneurial power' of 'flexible autocracy' in the Gulf states. Ennis, C. (2018), 'Reading Entrepreneurial Power in Small Gulf States: Qatar and the UAE', *International Journal*, 73(4): pp. 573–95, https://doi.org/10.1177/0020702018809980.
[27] Shires, J. (2019), 'Cybersecurity Governance in the GCC', in Ellis, R. and Mohan, V. (2019) (ed.), *Rewired: Cybersecurity Governance*, Wiley-Blackwell, p. 22.
[28] Shires, J. (2019), 'Family Resemblance or Family Argument? Three Perspectives of Cybersecurity and Their Interaction', *St Anthony's International Review*, May, 15(1).

revelations exposed US and allied cyberespionage in the region.[29] Nonetheless, the main state-sponsored cyberthreat to GCC states and organizations comes from Iran, in line with wider geopolitical cleavages.

Iran was the victim of the infamous Stuxnet virus targeting its nuclear enrichment facilities and has since then developed significant offensive cyber capabilities

Iran was the victim of the infamous Stuxnet virus targeting its nuclear enrichment facilities, attributed to the US and Israel, and has since then developed significant offensive cyber capabilities.[30] In addition to the Shamoon data deletion cyberattack against Saudi Aramco and RasGas in 2012,[31] and its reoccurrence across several Saudi government networks in late 2016 and early 2017,[32] Iran's focus in the GCC has been primarily on espionage, matching its broader cyber strategy.[33] Several sophisticated cyberespionage campaigns have been publicly attributed to Iranian state-linked actors since 2016, although the exact nature of state direction varies.[34] In the last two years, cybersecurity companies have identified Iran-linked campaigns targeting high-value government targets, including police, foreign ministries and intelligence agencies in the GCC and the Middle East more widely.[35]

In addition to the 'traditional' cyberthreats above, other elements of the information environment are a key aspect of cybersecurity in the GCC. Per capita wealth and internet penetration in the GCC are extremely high, although with significant intra-GCC and within-state variation.[36] In conjunction with explicit censorship and largely restrained traditional media, this has led to the GCC public sphere operating mainly on social media platforms, especially Twitter.[37] Such platforms have been used to both test and reinforce prevalent social norms on family relationships, religion and gender, as well as by international dissidents and refugees.[38] Social media has also been used by various factions in nearby conflicts, including by Islamic State of Iraq and Syria (ISIS), to recruit fighters and publicize atrocities, with messages directed at GCC populations as well as governments participating in military coalitions. Overall, because social media platforms were widely seen as contributing to the Arab Spring revolutions

[29] McAfee Labs (2011), *Global Energy Cyberattacks: 'Night Dragon'*, White Paper, https://www.heartland.org/_template-assets/documents/publications/29423.pdf (accessed 21 Feb. 2020); FireEye (2017), 'Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure', 14 December 2017, https://perma.cc/HVK5-2WGB; Kaspersky Lab (2015), 'Equation Group: Questions and Answers v1.5', Kaspersky Lab Global Research and Analysis Team, February 2015; Symantec Security Response (2015), 'Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance v1.1'; Rosenbach, M., Schmundt, H. and Stöcker, C. (2015), 'Source Code Similarities: Experts Unmask 'Regin' Trojan as NSA Tool', *Spiegel Online*, 27 January 2015, https://perma.cc/SEH5-YA94.

[30] Zetter, K. (2014), *Countdown to Zero Day*, New York: Penguin Random House.

[31] Bronk, C. and Tikk-Ringas, E. (2013), 'The Cyber Attack on Saudi Aramco', *Survival*, 55(2): pp. 81–96, https://doi.org/10.1080/00396338.2013.784468.

[32] Kaspersky Lab (2017), *From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond*, Kaspersky Lab Global Research and Analysis Team, 7 March 2017.

[33] Shires, J. (2018), 'Iran May Prioritise Cyber Espionage, Not Attack', *Oxford Analytica Daily Brief*, 11 July 2018. Although it is worth noting the report in Hope, B., Strobel, W. and Volz, D. (2019), 'High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran', *Wall Street Journal*, 7 August 2019, https://perma.cc/6ZYG-ET6H.

[34] Maurer, T. (2018), *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press; Anderson, C. and Sadjadpour, K. (2018), *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, Carnegie Endowment for International Peace.

[35] Shires, J. (2019), 'Iran Sharpens Cyber Tools for Foreign Policy Ends', *Oxford Analytica Daily Brief*.

[36] Hanieh, A. (2018), *Money, Markets, and Monarchies: The Gulf Cooperation Council and the Political Economy of the Contemporary Middle East*, New York: Cambridge University Press.

[37] See the recent collection of essays in the special issue Khamis, S. (2019), 'The Online Public Sphere in the Gulf: Contestation, Creativity, and Change', *Review of Middle East Studies,* 53(2): pp. 190–199; Murphy, E. (2009), 'Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere', *International Studies Quarterly,* 53(1): pp. 1131–53.

[38] Mohamed, E., Douai, A. and Iskandar, A. (2019), 'Media, identity, and online communities in the Arab world', *New Media and Society,* 21(5), https://doi.org/10.1177%2F1461444818821360.

and simultaneous protests in the GCC, monitoring and controlling social media became a key aspect of cybersecurity for GCC governments.[39]

Internationally, this double perception of cyberthreats matches the sovereign and controlled model of the internet put forward by Russia and China, among others, since the late 1990s.[40] The GCC countries all voted in favour of two Russian-sponsored resolutions in the UN General Assembly (UNGA) First and Third Committees in December 2018, one on cyber governance and one on cybercrime. The first one created an Open-Ended Working Group (OEWG) to study the existing norms contained in the previous UN Group of Governmental Experts (GGE) reports, identify new norms, and study the possibility of establishing regular institutional dialogue under the auspices of the UN.[41] The second one requests the secretary-general to present a report based on the views of member states on the challenges that they face in countering the use of information and communications technologies for criminal purposes for consideration by the General Assembly.[42] More recently, all GCC countries either voted in favour of or abstained (Saudi and Bahrain) from the newest Russian resolution on cybercrime, which would establish a committee of experts to consider a new UN cybercrime treaty.[43] Several states, including the US, have argued that the Russian treaty plan paves the way for an overly restrictive approach to dealing with cybercrime at the global level.[44] The GCC support of these resolutions, as well as their voting pattern in other UN discussions, suggests that they sit rather firmly within the 'cyber sovereignty' model of internet governance rather than a multi-stakeholder version.[45] GCC states have also sought to protect regional interests through internet governance mechanisms, for example by preventing the creation of .persiangulf as a top-level domain – as they objected to the geographical term – through legal action against ICANN.[46]

However, a clear divide between cyberthreats of intrusion and influence is difficult to maintain for two reasons. First, intrusion and influence can be combined through 'hack-and-leak operations'. Although the leaking of hacked emails from the US Democratic National Committee before the 2016 presidential election is the clearest recent example of this tactic, hack-and-leak operations came to prominence in the Gulf a year earlier, following the release of thousands of documents from the Saudi Ministry of Foreign Affairs by the Yemen Cyber Army in May 2015.[47] Hack-and-leak

[39] Matthiesen, T. (2013), *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring That Wasn't*, Stanford, California: Stanford University Press.
[40] Cornish, P. (2015), 'Governing Cyberspace through Constructive Ambiguity', *Survival,* 57(3): pp. 153–76.
[41] UN General Assembly Resolution A/C.1/73/L.27/Rev.1 on 'Developments in the field of information and telecommunications in the context of international security', 2018, https://undocs.org/A/C.1/73/L.27/Rev.1 (accessed 21 Feb. 2020).
[42] UN General Assembly Resolution A/C.3/73/L.9/Rev.1, on 'Countering the use of information and communications technologies for criminal purposes', https://undocs.org/A/C.3/73/L.9/Rev.1 (accessed 21 Feb. 2020).
[43] UN General Assembly Resolution A/C.1/73/L.27/Rev.1 on 'Developments in the field of information and telecommunications in the context of international security'.
[44] Hakmeh, J. and Peters, A. (2020), 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', Net Politics, Council on Foreign Relations, 13 January 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet (accessed 13 Jan. 2020).
[45] Shires, J. (2018), 'Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States', *War on the Rocks* (blog), 12 October 2018, https://perma.cc/L4CL-2B8A.
[46] Reed, L., Sabater, A. and van den Berg, A. J. (2016), 'Partial Final Declaration of the Independent Review Process Panel', GCC (Claimant) and ICANN (Respondent), *International Center for Dispute Resolution*, 19 October 2016.
[47] Shires, J. (2019), 'Hack-and-Leak Operations: Intrusion and Influence in the Gulf,' *Journal of Cyber Policy,* 4(2): pp. 235–56.

operations were then a central feature of the June 2017 Gulf crisis, where the 'quartet' states of Bahrain, Egypt, Saudi Arabia and the UAE blockaded Qatar due to accusations of support for terrorist organizations.[48]

Second, as argued in the previous section, due to the increasing strategic use of both intrusion and influence operations, the US and other multi-stakeholder proponents have also moved to defend their national 'information space' and protect their national communications technology companies. While we do not intend to imply a false equivalence between these actions and extensive internet censorship and control, these shifts have made it harder to separate analytically two clearly polarized approaches to internet governance. Instead, the double threat perception of the GCC states is thus now shared by many other states. Consequently, this paper takes a comprehensive approach to cyber resilience that recognizes this double threat perception, including both resilience to 'traditional' cyberattacks and to attempts to influence the information environment in a state.

The state of cybersecurity in the GCC: An overview

All GCC states have long-term national plans that seek to refocus their economies from extractive industries towards technology and innovation

All GCC states have long-term national plans that seek to refocus their economies from extractive industries towards technology and innovation, reduce the role of the public sector, and reduce high expatriate numbers through extensive training and preferential treatment for citizens.[49] Following these national plans, GCC states have taken significant steps to digitize government services, with the UAE ahead of the others in many respects. Following early attention garnered by Dubai's e-government measures in the mid-2000s, and extensive collaboration with international consultants in 2013 and 2014, the UAE occupied 34th position in the 2017 Waseda International Digital Government Rankings, with especially high scores in the promotion of digital government (9th) and e-participation (7th).[50]

In the context of digitizing their governments and societies, the GCC states have all adopted measures aimed at increasing cyber resilience and at upgrading cybersecurity capacity. According to the ITU Global Cybersecurity Index (GCI), Saudi Arabia, Oman and Qatar score highly, ranking as the top three countries of the Arab world on the index.[51] The following three states from the region were the UAE, Kuwait and Bahrain. The ITU index measures elements of state cybersecurity based on a range of legal, organizational, technical, capacity-building and cooperation measures. Although the ITU's index results are often questioned, given that they rely on self-assessment by states, the positions that the GCC states occupy on the index are nonetheless significant and show the resources and investment that these countries have put in so far compared to the rest of the Arab states.[52]

[48] Shires, J. (forthcoming), 'The Cyber Operation against Qatar News Agency,' in Zweri, M. (ed.), *The Gulf Crisis: Origins, Implications, Repercussions*, Berlin Heidelberg: Springer Nature.
[49] Bahrain National Plan 2030, Kuwait Vision 2035, Oman Vision 2040, Qatar Vision 2030, Saudi Arabia Vision 2030, and UAE Vision 2021.
[50] Buhumaid, H., Constantin, M. and Schubert, J. (2016), *How the UAE Government Modernized Citizen Services* McKinsey, May 2016, https://perma.cc/Y8RG-8USZ.
[51] ITU (2018), *Global Cybersecurity Index (GCI) 2018*, www.itu.int/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed 21 Feb. 2020).
[52] Shires, J. (2019), 'Cybersecurity Governance in the GCC', p. 23.

Table 1: GCC ranking on ITU's Global Cybersecurity Index for 2018

Country	Score	Regional rank	Global rank
Saudi Arabia	0.881	1	13
Oman	0.868	2	16
Qatar	0.860	3	17
UAE	0.807	4	33
Kuwait	0.600	5	67
Bahrain	0.585	6	68

Source: Compiled by authors from ITU, Global Cybersecurity Index 2018.

The ITU index illustrates how GCC states have taken many measures to improve their cybersecurity posture (see Table 2). As detailed in previous papers in this series, all GCC states have developed national cybersecurity strategies and introduced or revamped their cybercrime and electronic transaction legislation. Some states have also introduced national data protection legislation. The GCC states have all created dedicated cybersecurity organizations building on earlier computer emergency response teams (CERTs). Regarding standards, the GCC Standardization Organization lists Arabic versions of the ISO 27001 cybersecurity standard published in 2009 and 2015, respectively. Notably, the UAE national cybersecurity agency, established in 2012, has also published its own cybersecurity regulatory framework, the Information Assurance Standards (IAS), based on ISO 27001 versions 2005, 2013, and the US NIST 2014 cybersecurity framework.[53] The level of cybersecurity expertise is also increasing, with many universities offering undergraduate and graduate qualifications in technical and organizational aspects of cybersecurity, and significant take-up of these courses, especially by female students. Finally, the GCC states have all engaged in extensive wider education efforts, especially in child online protection in Oman and Saudi Arabia, and some regional cooperation at a GCC and Arab-state level, as well as with longstanding military partners in the US and Europe.

Overall, GCC states seek to be front-runners in digital innovation and so are vulnerable to an increasing range of cyberthreats. GCC governments have invested significantly in cybersecurity, especially since the landmark Shamoon cyberattack in Saudi Arabia and Qatar in 2012.

[53] This agency was called the National Electronic Security Authority (NESA) until early 2017, and is now called the Signals Intelligence Agency (SIA). Part of the reason for this re-organization involves the relationship between offensive and defensive cyber capabilities discussed in the following section.

Table 2: Government cybersecurity measures taken in the GCC

Measure	Bahrain	Kuwait	Oman	Qatar	KSA	UAE
Cybercrime law[54]	2014	2015	2011	2014	2015	2012
Data protection law[55]	2018	–	–	2016	–	–
Cybersecurity strategy[56]	2017	2017	2010	2014	2013	2019
Cybersecurity organization[57]	MOI/IeGO/ TRA	CITRA	OCERT	QCERT	NCSC	TRA

Source: Compiled by the authors.

However, there is more work still to be done in all the above areas. Despite the positive and unified picture portrayed in GCC cybersecurity strategies, they lack detail and remain very high-level, creating an image of a coherent approach without specifying clear guidance for individuals and organizations.[58] For cybersecurity organizations, publicly available information on their services is limited, impeding them from playing their expected role of promoting effective IT security practices and in creating a culture of cyber awareness and hygiene.

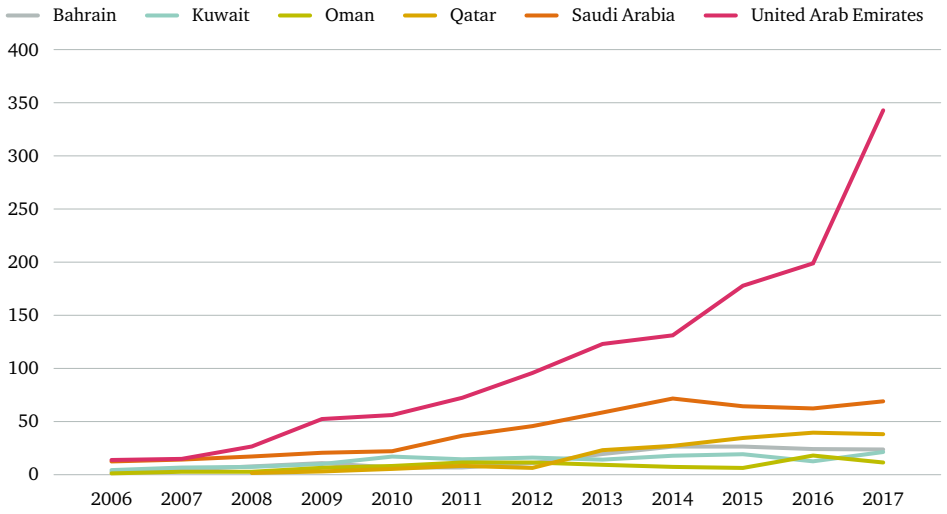
Moreover, these organizations have shifting and overlapping areas of responsibility: for example, at a national level the relative power of Saudi Arabia's National Cybersecurity Authority (NCA), the Saudi Federation for Cybersecurity, and National Cyber Security Center (NCSC) have changed significantly in the past three years, while, in the UAE, Dubai's independent cybersecurity authorities and regulations have not always been coordinated with governmental initiatives in Abu Dhabi. In Bahrain and Qatar, even where there is a responsible cybersecurity organization its relative responsibilities in relation to the Ministry of Interior are not always clear, and operational activity still resides in the latter. In their review of several states' cyber readiness, the Potomac Institute for Policy Studies reported that Saudi Arabia (the only GCC state included in the review) was 'still insufficiently prepared in all essential elements of cyber readiness' in 2017.[59]

Although the ITU Index accurately captures government regulations in relation to cybersecurity, it does not measure the implementation of key standards and regulation in both the public and private sectors. To gain a better understanding, this paper analyses implementation in the GCC using the available data, beginning with an overview of technical standards and data protection regulation, and then examines the finance, health and energy sectors – considered to be the key national infrastructure sectors in the GCC countries.

[54] Earlier versions of cybercrime laws were published in Oman (2001), Saudi Arabia (2007) and the UAE (2006).
[55] The Bahrain law concerns 'consumer protection for communications services'. The UAE and Saudi Arabia have data protection legislation for specific sectors, as below, while Dubai issued a Data Dissemination Law in 2016. Oman issued a regulation in 2009 on 'User data and privacy protection' for telecommunications companies, with similar language to the data protection laws in Qatar and Bahrain including cross-border controls, but it is not included here due to its narrow scope.
[56] Earlier versions of the Oman e-government strategy were published in 2003, the Saudi Arabia strategy in 2011, and the UAE strategy in 2014 and 2018.
[57] Bahrain's cybersecurity authority was formerly named the Central Informatics Organization (2002), Saudi Arabia's was formerly the National Electronic Security Centre (2013) and the Cyber Security Federation, while the UAE formed the National Electronic Security Authority in 2012 (see footnote 53 above).
[58] Shires, J. (forthcoming), 'Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf', in Broeders, D. (ed.), *Responsible Behaviour in Cyberspace*, London: Rowman & Littlefield Publishers, Inc.
[59] Hathaway, M., Spidalieri, F. and Alsowailm, F. (2017), *Kingdom of Saudi Arabia: Cyber Readiness at a Glance*, Potomac Institute, p. 23.

For technical standards, ISO conducts an annual survey to measure the implementation of key standards including 27001 (in both 2005 and 2013 versions), illustrated in Figure 1. ISO 27001 is the international standard for information security management systems. It comprises a set of measures aimed at achieving protection and preservation of an organization's information in line with the principles of confidentiality, integrity and availability. This survey shows that the number of ISO certificates has grown gradually in the GCC in this period, although it stayed static (and in Oman, declined) around 2013, potentially due to the introduction of the newer version of the ISO standard. The UAE is far ahead of the rest of the GCC in ISO certification, although Qatar has a high number of certificates given its small size.

Figure 1: ISO 27001 (2005) certificates 2006–17 in the GCC



Source: ISO (n.d.), 'The ISO Survey', https://www.iso.org/the-iso-survey.html.

ISO also tracks the number of sites where ISO 27001 applied between 2007 and 2015 (the last year for which data is available).[60] This data also shows an increase in this period, although with declines in the UAE, Saudi Arabia and Oman after 2013, again potentially due to the new version of the standard. Other surveys suggest that implementation of ISO cybersecurity standards is uneven in the GCC. An academic survey of ISO 27001 in Saudi Arabia in 2014 found that standards were low on security professionals' priorities, below personnel issues like training, expertise or salary, and organizational ones such as management involvement.[61] This suggests that, despite the impressive educational opportunities in cybersecurity in the GCC, these skills are not always translated into professional practice. Overall, the GCC has adopted international cybersecurity standards slowly and unevenly, and with many businesses focused on older versions of these standards after newer ones are available.

[60] Available at ISO (n.d.), 'The ISO Survey', https://www.iso.org/the-iso-survey.html.
[61] Alshitri, K. and Abanumy, A. N. (2014), 'Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia', in *2014 International Conference on Information Science Applications (ICISA)*, pp. 1–4, https://ieeexplore.ieee.org/document/6847396 (accessed 21 Feb. 2020).

For data protection regulation, in media interviews some cybersecurity professionals claimed that only 30–35 per cent of UAE companies would be compliant with European data protection standards (GDPR), and around half that number were even aware of the steps necessary for compliance.[62] A survey by a data storage solution provider, including 100 respondents in the UAE, highlighted the existence of large amounts of data in organizations that could contravene GDPR requirements.[63] Separately, Gulf Business Machines (GBM) has conducted an annual survey of 'IT/security managers and professionals' in the GCC since 2014 (the last year for which data is available is 2017), with the number of respondents varying between around 600 and 1,500.[64] The survey is presented as an independent analysis of the cybersecurity community, although the results are shown in a way clearly designed to market GBM products. Despite this bias, its sample size and repetition make it a valuable source in an area of limited data. This survey suggests that cybersecurity capacity is slowly increasing in the private sector, as 43 per cent of enterprise respondents claimed they had the capabilities to predict and prevent cyberattacks in 2015, rising to 50 per cent in 2016; similarly, 58 per cent claimed they had an effective security strategy in 2015, rising to 79 per cent in 2017.

43 per cent of enterprise respondents claimed they had the capabilities to predict and prevent cyberattacks in 2015, rising to 50 per cent in 2016

For finance, digital financial transactions are governed by e-transaction and e-commerce laws introduced throughout the GCC between 2002 (UAE) and 2014 (Kuwait). There are several free-trade zones in the GCC that operate under different financial regulations to the rest of the state, the most notable being the Dubai International Financial Centre (DIFC), the Abu Dhabi Global Market (ADGM) and the Qatar Financial Centre (QFC). These centres also have different cybersecurity regulations, mainly focusing on data protection: DIFC is regulated by a data protection law introduced in 2005, amended in 2012; ADGM's data protection regulation was introduced in 2015 and amended in 2018 (with an Office of Data Protection established in 2017); and the QFC has had separate data protection regulation since 2005. These regulations aim to ensure that businesses in these free-trade zones are able to work internationally, and so they explicitly claim to follow international regulations, especially that of the European Union. However, financial regulation – including on data disclosure requirements – has been insufficient to prevent the inclusion of the UAE and Oman on an EU list of 17 countries, finalized in March 2019, which either failed to comply with required financial 'good-governance' criteria or did not commit to doing so.[65]

For health, the UAE has introduced Federal Law no.2 2019 for healthcare data, while Dubai's Healthcare City has had separate data protection regulation since 2013. In Saudi Arabia the transfer of financial and health information is regulated by the relevant sector bodies. The other GCC states do not have separate healthcare cybersecurity regulation.

[62] Cherrayil, N. (2018), 'Many UAE Firms Will Miss General Data Protection Regulation Deadline', *Gulf News*, 17 May 2018, https://perma.cc/D5QC-XWCM.
[63] Veritas (2018), '81% of Data Stored by UAE Organisations Is Unclassified Despite Improvements in Data Management', https://perma.cc/4Q5K-H98A.
[64] GBM (2016), *Annual Security Survey*, 5th edition; GBM (2017), *The Evolution of GCC Enterprises: Are They Ready for the next Generation?* 6th Annual Security Survey, https://perma.cc/WPZ7-5QMN; GBM (2018), *Breached or Not Breached? Exploring the Shift from Prevention towards Detection and Response in the Gulf Region*, 7th Annual Security Survey (separate survey in Qatar).
[65] Dendrinou, V. and Pronina, L. (2019), 'U.A.E., 9 Other Jurisdictions Added to EU Tax-Haven Blacklist', *Bloomberg.Com*, 12 March 2019, https://perma.cc/Q59Y-Y6KG.

Given the GCC 'late rentier' economic model, cybersecurity threats to the oil and gas sector are particularly concerning for national governments.[66] Companies in this sector have extra cybersecurity responsibilities due to their crucial role in the functioning of the state and as a core economic foundation for both international stability and national welfare. There have been several notable cyberattacks against the oil and gas industry in the GCC, including the Shamoon incident in 2012, and more recently malware that altered the settings of industrial control safety systems in a Saudi petrochemical and refining complex in 2017, with the potential to disrupt production and harm employees.[67] Cybersecurity provision in the energy sector, and oil and gas in particular, has three particular challenges, in addition to the wider issues above.[68] First, there is an economic incentive for companies to adopt IP-based operational technology networks for more efficient production, creating practical problems in isolating such networks from their internet-connected business networks. Second, the cybersecurity priority for these companies is protection from espionage (corporate or state-sponsored), rather than damage, as the former is seen as a more immediate threat to their business model and reputation. Third, like other industries, the oil and gas sector has a long and complicated supply chain, with many vulnerabilities introduced early on, so transferring good practices down the supply chain is difficult.

Overall, the uneven nature of cybersecurity provision in the GCC states means that it may be difficult for these states to recover from a large-scale cyber incident. GCC states need to improve their cyber resilience as well as their cybersecurity in order to withstand and rapidly recover from cyber disruption.

An imbalance towards centralized cyber resilience

The first element of centralization against information threats is cybercrime legislation. A cybercrime law that is fit for purpose should consist of a substantive part (elaborating on the crimes and sanctions in case of breach of the law) and a procedural part (elaborating on the processes to be followed in a cybercrime investigation, prosecution and adjudication). GCC cybercrime laws in their current form do not serve that purpose. Instead, they focus on content, expanding the definition of cybercrime to a wide array of acts using vague language that covers a large number of actions.[69] These acts include but are not limited to insulting or defaming religion or religious values, invading privacy, damaging the state's reputation, criticizing the ruler, his family or a public official and changing or overthrowing the ruling regime. Consequently, by focusing on criminalizing these acts, these laws have played more of a role in restricting online speech rather than in combating cybercrime.[70]

---

[66] Gray, M. (2011), 'A Theory of 'Late Rentierism' in the Arab States of the Gulf', *Center for International and Regional Studies,* Occasional Paper No. 7, Georgetown University, https://repository.library.georgetown.edu/bitstream/handle/10822/558291/CIRSOccasionalPaper7MatthewGray2011.pdf (accessed 21 Feb. 2020).

[67] FireEye (2017), 'Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure'; Newman, L. H. (2018), 'Russia Has Been Linked to Malware That Targets Industrial Equipment', *Wired*, 23 October 2018, https://perma.cc/CGD6-FX85.

[68] This paragraph draws on a report written by one of the authors, based on a survey conducted by the Ponemon Institute, Siemens Middle East (2018), *Assessing the Cyber Readiness of the Middle East's Oil and Gas Sector*, Ponemon Institute.

[69] For an extensive discussion on this topic see, Hakmeh, J. (2018), *Cybercrime Legislation in the GCC Countries: Fit for Purpose?*.

[70] There is no universally agreed definition of the term 'cybercrime'. For the purposes of this paper, the same approach is followed as in the Budapest Convention in defining the term cybercrime as any offence or collection of offences falling under at least one of the following categories: (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer-related offences; (iii) content-related offences; and (iv) offences related to infringements of copyright and related rights.

Furthermore, legislative tools for controlling online speech are not restricted to cybercrime laws. Penal codes across the GCC include various clauses on *lese majeste* and respectful behaviour on moral, family and religious subjects, and have been applied to social media comments.[71] Offline media laws have been extended to cover social media, notably in Kuwait's e-media law of 2016. Counterterror laws have also been used to control a wide range of social media content, with the justification that any dissident and controversial opinion could provoke violence and unrest. Even with these legislative tools, identifying social media users relies on centralized surveillance capabilities detailed below.[72]

Second, governments have mobilized the affordances of social media platforms themselves to prevent popular expressions of dissatisfaction. Research indicates that Saudi Arabia and the UAE use large networks of automatically created accounts (botnets) to follow and retweet *en masse*.[73] This technique can be used to support government or approved public figures, to counter anti-government views, or simply to distract attention from certain individuals or groups. These botnets were especially active following the Qatar split in 2017. In Saudi Arabia, open source investigations indicate that one individual, Saud Al Qahtani, was largely responsible for this social media control strategy, which was linked to cases of detention and mistreatment.[74] In a clear example of centralization, Al Qahtani reportedly used his positions as head of the Saudi Federation for Cybersecurity, and in the Royal Court as head of the 'Cybermedia Group', to exert influence over social media in Saudi Arabia.

The telecoms sector is another way in which information threats are managed in a highly centralized manner.[75] Although the GCC telecoms sector was privatized in the early 2000s, with a single national entity split into two or three, most companies retained a substantial government share and close links to security organizations.[76] National telecoms laws and regulatory agencies mandate government access for national security reasons.[77] Consequently, national telecoms companies play a key role in national monitoring and filtering due to their control of internet traffic over national borders, and outsource this responsibility to other companies.[78] In addition to traffic management and analysis and the censorship of specific websites or content, telecoms

[71] Shires (forthcoming), 'Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf'.
[72] Although some media reports indicate that the Saudi Arabian government has used Twitter employees and consultants to police social media. Benner, K., Mazzetti, M., Hubbard, B. and Isaac, M. (2018), 'Saudis' Image Makers: A Troll Army and a Twitter Insider', *The New York Times*, 20 October 2018, https://perma.cc/E84Q-BK9S.
[73] Leber, A. and Abrahams, A. (2019), 'A Storm of Tweets: Social Media Manipulation During the Gulf Crisis', *Review of Middle East Studies*, pp. 1–18, https://doi.org/10.1017/rms.2019.45; Jones, M. O. (2019), 'Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis', *International Journal of Communication,* 13(27); Cherkaoui, T. (2018), 'A New Kind of Information Warfare? Cyber-Conflict and the Gulf Crisis 2010–2017', *The Political Economy of Communication,* 6(1).
[74] b33lz3bub (2019), 'Lord Of The Flies: An Open-Source Investigation Into Saud Al-Qahtani', *bellingcat*, 26 June 2019, https://perma.cc/M6AQ-992J.
[75] It should be noted that the practice, employed throughout the GCC, of enabling citizens to *recommend* websites for blocking is an example of a distributed response to an information threat, and thus runs counter to the trends identified in this section more generally.
[76] Thompson, B. (2009), 'UAE Blackberry Update Was Spyware', *BBC News*, 21 July 2009, https://perma.cc/97UP-3APN.
[77] For example, Telecommunications Regulatory Authority (Oman), 'Royal Decree No. 30/2002 Telecommunications Regulatory Act' (Government of Oman, 2003); Telecoms Regulatory Authority (Bahrain), 'The Telecommunications Law of the Kingdom of Bahrain' (Government of Bahrain, 23 October 2002); ictQatar, 'Telecommunications Law – Decree Law No.34 of 2006' (Government of Qatar, 2006).
[78] Haselton, B. (2013), 'Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE', *Citizen Lab*, 28 November 2013; Dalek, J., Gill, L., Marczak, B., McKune, S., Noor, N., Oliver, J., Penney, J., Senft, A. and Deibert, R. (2018), 'Planet Netsweeper', *Citizen Lab*, 25 April 2018; Marquis-Boire, M., Dalek, J., McKune, S., Carrieri, M., Crete-Nishihata, M., Deibert, R., Khan, S., Noman, H. Scott-Railton, J. and Wiseman, G. (2013), 'Planet Blue Coat: Mapping Global Surveillance and Censorship Tools', *Citizen Lab*, January 2013.

companies often use specialized equipment to block Voice over IP (VOIP) services such as Skype, encrypted messaging, encrypted VOIP, and virtual private networks (VPNs). Motivations for the blocking are open to speculation, with possible reasons including the size of the expatriate community in the GCC countries and the desire to protect the revenues resulting from international calling, in addition to official concerns over security issues arising from the use of unlicensed over-the-top applications (OTT) (such as WhatsApp, Skype, Facebook Live, etc.) calling and content distribution channels. Evidently, however, there is an overlap between commercial and security motivations for such blocking.[79]

GCC states have acquired and used offensive cyber capabilities from the private sector and centralized the underlying intelligence and surveillance infrastructure on which these capabilities depend

GCC states have themselves acquired and used offensive cyber capabilities from the private sector and centralized the underlying intelligence and surveillance infrastructure on which these capabilities depend. In 2012, the *Washington Post* reported that US defence company Booz Allen Hamilton had been requested by the Qatari government to provide a cyber operations centre to conduct hacking operations against its regional adversaries.[80] Separately, Raytheon's 'Intelligence and Information Systems Division' played the role of 'integrator' for the UAE's then-National Electronic Security Agency (NESA) since its founding in 2012.[81] Although Raytheon was the main contractor for the UAE government, reports suggest that Raytheon subcontracted much of the work to US technology company Cisco and Booz Allen Hamilton, and that US company Verint later took over the contract (more recent reorganizations have created NESA's successor, the Signals Intelligence Agency (SIA)). Separately, a BBC investigation in 2017 reported that Danish company ETI, acquired by BAE Systems in 2010, had sold national-level surveillance technologies to Saudi Arabia, UAE, Qatar and Oman.[82] Moreover, since the Arab Spring protests, Bahrain has developed technologies to identify the IP address of social media users, which has also been used to detain individuals.[83]

More targeted offensive cyber capabilities have been reportedly used by GCC governments, including technologies sold by: Italian company Hacking Team (in which a Saudi-controlled company has a significant stake)[84] in all GCC states other than Kuwait and Qatar; German-British company Finfisher in all GCC states other than Kuwait; and Israeli company NSO Group in the UAE and Saudi Arabia.[85] These technologies include expensive exploits of widespread and difficult-to-detect vulnerabilities; consequently, their use increases cybersecurity risks overall. There has been significant publicity around these technologies due to their presence on the devices of dissidents and

[79] Dajani, H. (2016), 'UAE Telecoms Regulator Defends Decision to Block Snapchat Calling', The National, 12 April 2016, https://perma.cc/STL9-SLV5; Unknown (2017), 'Out of Sight, out of Mind? Blocking Doha News in Qatar', *Journal of Middle Eastern Politics and Policy*, 12 January 2017, https://perma.cc/UX6E-KMB2; Marlinspike, M. (2013), 'A Saudi Arabia Telecom's Surveillance Pitch', 13 May 2013, https://moxie.org/blog/saudi-surveillance/ (accessed 21 Feb. 2020).
[80] Nakashima, E. (2012), 'As Cyberwarfare Heats up, Allies Turn to U.S. Companies for Expertise', *Washington Post*, 22 November 2012, https://perma.cc/WNP6-UUS3.
[81] *Intelligence Online* (2017), 'Verint Poised to Land Major Emirates Interceptions Contract', 18 October 2017, https://perma.cc/W6Q9-M6G5; *Intelligence Online* (2017), 'Abu Dhabi's NSA and Its Helping Hands', 5 April 2017, https://perma.cc/PTH3-AYXU.
[82] *BBC News* (2017), 'How BAE Sold Cyber-Surveillance Tools to Arab States', 15 June 2017, https://perma.cc/75ZM-NXYD.
[83] Bahrain Watch (2013), 'The IP Spy Files: How Bahrain's Government Silences Anonymous Online Dissent', 1 August 2013, https://perma.cc/U4PX-JC6P.
[84] Franceschi-Bicchierai, L. (2018), 'Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia', *Motherboard*, 31 January 2018, https://perma.cc/ZR94-TANK.
[85] Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. and Deibert, R. (2018), 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', *Citizen Lab,* 18 September 2018; Marczak, B., Guarnieri, C., Marquis-Boire, M. and Scott-Railton, J. (2014), 'Mapping Hacking Team's 'Untraceable' Spyware', *Citizen Lab*, 17 February 2014; Marczak, B., Scott-Railton, J., Senft, A., Poetranto, I. and McKune, S. (2015), 'Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation', *Citizen Lab*, 15 October 2015.

activists worldwide, including contacts of murdered journalist Jamal Khashoggi.[86] Other offensive cyber companies for hire in the Gulf include less well-known South Asian contractors.[87] In particular, there are companies in the UAE that blur the lines between offensive capability and benign cybersecurity protection. For example, Dark Matter provides cybersecurity solutions to industry and government, and was reportedly involved in large-scale telecoms interception and targeting of individuals deemed to be a threat.[88] One report, by a former NSA and Dark Matter employee, suggested these targets included US citizens.[89] This activity led Mozilla to withdraw certificate signing permission for the Firefox browser from Dark Matter in July 2019, thereby undermining a potential cybersecurity improvement.[90] Other than the proliferation of the use of spyware to conduct offensive cyber operations, the 2017 GCC split itself may have occurred due to an offensive cyber operation using a different approach. Several media reports indicated that contractors working for the UAE had altered the website of the Qatar News Agency to insert pro-Iran comments prior to the crisis.[91]

Overall, the GCC approach to its internet environment is extremely centralized, providing resilience against perceived threats to political stability, especially on social media. This centralized approach cements the idea of a national information environment itself, as opposed to a supposedly free flow of information on the global internet. However, this centralization often has clear negative consequences for human rights, especially those connected to privacy and freedom of expression. Furthermore, a centralized approach focusing on content control can actively reduce cybersecurity provision for individuals and organizations more widely. In sum, the GCC states have over-emphasized centralized over distributed approaches to cyber resilience, due to their emphasis on control of the information environment.

Technological factors affecting future resilience

There are four wider developments in internet technologies relevant to cyber resilience in the GCC.[92] First, the development of a digital economy.[93] E-commerce will continue to increase across the GCC, with online platforms such as Noon and Souq (acquired by Amazon) moving transactions online. App-enabled delivery and ride-hailing companies are now available in some areas of the GCC, with the most popular Middle East ride-hailing app, Careem, recently acquired by its competitor Uber. There are also payment innovations, especially in previously cash-dependent economies, for example,

[86] Barnes, J. E. (2018), 'C.I.A. Concludes That Saudi Crown Prince Ordered Khashoggi Killed', *The New York Times*, 17 November 2018, https://perma.cc/KG6E-UNYA.
[87] Anderson, C. and Guarnieri, C. (2017), 'Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia', *bellingcat*, 27 October 2017, https://perma.cc/V57A-66MU; Amnesty International (2017), 'Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal', 14 February 2017.
[88] Margaritelli, S. (2016), 'How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People', 27 July 2016, https://perma.cc/EDD3-Y9RZ.
[89] Bing, C. and Schectman, J. (2019), 'Exclusive: Ex-NSA Cyberspies Reveal How They Helped Hack Foes of UAE', *Reuters*, 30 January 2019, https://perma.cc/38Z9-XT48.
[90] Bing, C. and Schectman, J. (2019), 'Mozilla Blocks UAE Bid to Become an Internet Security Guardian.', *Reuters*, 9 July 2019, https://perma.cc/P9J3-E42H.
[91] DeYoung, K. and Nakashima, E. (2017), 'UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials', *Washington Post*, 16 July 2017, https://perma.cc/TJ8D-8ZSE.
[92] Although this section focuses on technological change, we recognize that social factors influence technological adoption and seek to avoid a simple technological determinism.
[93] For further discussion, see Mogielnicki, R. (2019), 'Add to Cart: E-Commerce Development in the Gulf', *Arab Gulf States Institute in Washington* (blog), 18 December 2019, https://agsiw.org/add-to-cart-e-commerce-development-in-the-gulf/ (accessed 21 Feb. 2020).

several mobile and quick card payment systems are gradually spreading in Saudi Arabia. There are many entrepreneurs in the region seeking to stimulate investment in the digital sector, such as the online investment platform Magnitt in Dubai. Many businesses in the GCC rely on cloud computing, with data on servers across the GCC and internationally. However, despite an ITU report in 2016 calling for an 'Arab Safe Harbor' agreement to regulate cloud storage and enable a cloud-based digital economy, this has not been implemented.[94] Overall, an increasingly digital economy creates a wider range of cybersecurity risks, especially for identity fraud and theft, as areas of individuals' lives and organizations' activities are potentially affected by malicious activity on networks and devices.[95]

Industry reports suggest a low level of 5G readiness more broadly, as 5G adoption depends on the development of appropriate devices and services as well as the networks themselves

Second, the adoption of 5G telecoms networks will also have a significant impact on cybersecurity in the GCC. Within days of each other, GCC states, including the UAE, Qatar and Saudi Arabia, all claimed to be the first worldwide to implement 'live' 5G networks.[96] Despite these claims, industry reports suggest a low level of 5G readiness more broadly, as 5G adoption depends on the development of appropriate devices and services as well as the networks themselves.[97] Elsewhere, 5G cybersecurity has been framed around the risk of access by hostile governments: for example, US President Donald Trump has issued an executive order banning US companies from using information and communications technology from any provider considered a national security threat.[98] This executive order was primarily targeted against Huawei due to concerns over its links to the Chinese state and potential espionage.[99] While Chinese companies are investing in 5G in the GCC (through Huawei, OPPO, and other firms),[100] there has been little public debate about the relative benefits of this involvement in a manner akin to that in Europe, Australia and the US, and so the cybersecurity risks are either not well captured or they are accepted as a trade-off for the competitive pricing of Chinese 5G infrastructure.

Third, the Internet of Things (IoT) also changes the cybersecurity landscape in the GCC. The IoT increases the attack surface for malicious cyber activities, as many more points of entry exist into home and corporate networks and IoT manufacturers have low incentives to secure their devices rather than prioritize market speed and flexibility.[101] The IoT is still a future development for much of the GCC, although contracts have been signed to provide specific satellite infrastructure, and some market reports claim that up to half of hospitals in Qatar, the UAE, and Saudi Arabia

[94] Alamir Ali, R. (2016), *Cloud Computing in Arab States: Legal Aspect, Facts and Horizons,* ITU Arab Regional Office.
[95] Benni, E., Elmasry, T., Patel, J. and aus dem Moore, J. P. (2016), 'Digital Middle East: Transforming the Region into a Leading Digital Economy', McKinsey & Company.
[96] Ooredoo (2018), 'Ooredoo First In The World to Launch 5G Commercial Network', *CISTON PR Newswire*, 14 May 2018, https://perma.cc/73D6-7X3L; Langton, J. (2018), 'Etisalat Prepares to Offer Customers Ultra-Fast 5G Network', *The National*, 14 May 2018, https://perma.cc/W4QS-PTMG; Debusmann Jr, B. (2018), 'Saudi Arabia's Al Khobar Becomes First Middle East City to Test 5G', *ArabianBusiness.com*, 27 May 2018, https://perma.cc/Q6T4-ZMD4.
[97] Iacopino, P., Robinson, J. and Meloan, M. (2018), '5G in MENA: GCC Operators Set for Global Leadership', GSMA Intelligence, https://www.gsmaintelligence.com/research/2018/11/5g-in-mena-gcc-operators-set-for-global-leadership/709/ (accessed 21 Feb. 2020).
[98] Liu, N., Sevastopulo, D. and Stacey, K. (2019), 'Donald Trump Issues Executive Order Laying Ground for Huawei Ban', *Financial Times*, 15 May 2019, https://www.ft.com/content/c8d6ca6a-76ab-11e9-be7d-6d846537acab (accessed 21 Feb. 2020).
[99] Mueller, M. (2019), 'Let's Have an Honest Conversation about Huawei', *Internet Governance Project* (blog), 16 October 2019, https://www.internetgovernance.org/2019/10/16/lets-have-an-honest-conversation-about-huawei/ (accessed 31 Jan. 2020).
[100] Telecom Review (2019), 'Chinese Firm Announces 5G Investment Plans in GCC', 16 January 2019, https://perma.cc/KRE5-CU4X.
[101] Bryce, H. (2017), 'The Internet of Things Will Be Even More Vulnerable to Cyber Attacks', Chatham House Expert Comment, 18 May 2017, https://www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks (accessed 24 Feb. 2020).

use IoT solutions.[102] Cybersecurity professionals in the GCC recognize these risks: for example, Ooredoo (in Oman and Qatar) has joined a not-for-profit aiming to increase awareness of cybersecurity risks in IoT and encourage secure standards.[103] The UAE's Telecommunication Regulatory Authority (TRA) has published a new policy aimed at regulating the services and devices associated with IoT.[104]

Fourth, and finally, artificial intelligence (AI) and machine learning are technological fields with deep implications for cyber resilience in the GCC. The importance of big data for AI exacerbates existing cybersecurity risks to individuals, businesses and governments from the deletion, manipulation, and theft of valuable data. On the other hand, AI itself provides an exciting new avenue for research and product development in cybersecurity, offering the promise of scalable real-time threat detection and increasingly automated responses. In October 2017, the UAE adopted a minister for AI to signal its commitment to the adoption of these technologies, especially in the planned smart cities of Dubai and Abu Dhabi.[105] Saudi Arabia has made AI a cornerstone of its announcements in a range of technological plans, including the new city NEOM and the Future Investment Initiative.[106] However, so far there is no evidence of a substantial technological shift with cybersecurity implications over and above these announcements.[107]

AI itself provides an exciting new avenue for research and product development in cybersecurity

These technological changes will have as yet unknown implications for cyber resilience, especially in the context of extensive international competition between global powers such as the US and China for control of resources and knowledge in most of these areas. However, these changes can be grouped into three main areas.

First, will AI or IoT leadership lead to new privacy demands or violations, especially in GCC-led adoption of smart cities? Will data be the new oil in the GCC and what approach to data governance, storage and use will the region adopt? How will ownership of the region-specific and global datasets required for training competent AI algorithms affect state power and private-sector relationships?

Second, will the trade-off between economic benefit and risks of espionage in 5G and AI, exemplified by current US pressure on its European allies, apply to the GCC states in the future? If required to choose, will they remain under its security umbrella and continue investing in US companies, or will they embrace China in a 'pivot' that may be both ideologically aligned and economically beneficial?

Third, and finally, if the GCC states become leaders in these technologies, as intended, what are the implications for cyber risks? How will this change regional competition,

[102] ORBCOMM (2016), 'ORBCOMM and Machinestalk Deliver IoT Solutions in Saudi Arabia and The GCC Region', ORBCOMM, 18 May 2017, https://perma.cc/75MB-CNL4; Fernando, C. (2016), 'Internet of Things Set to Go Mainstream in GCC Hospitals', ChannelPostMEA, 26 December 2016, http://www.channelpostmea.com/2016/12/26/internet-of-things-set-to-go-mainstream-in-gcc/ (accessed 21 Feb. 2020).
[103] CommsMEA Staff Writer (2018), 'Ooredoo Oman Joins LoRa Alliance to Drive IoT', CommsMEA, 2 April 2018, https://perma.cc/3B3X-G43B.
[104] Telecommunications Regulatory Authority (UAE) (2018), 'Regulatory Policy: Internet of Things (IoT)', 22 March 2018, https://www.tra.gov.ae/assets/8oQGhqPt.pdf.aspx (accessed 21 Feb. 2020).
[105] UAE Government (2017), 'UAE Strategy for Artificial Intelligence', Government.ae, https://perma.cc/TJ5G-EDT8; Zakaria, S. (2017), 'Dubai's Smart Lab Accelerates AI Move', *Khaleej Times*, 27 March 2017, https://perma.cc/J3LA-LGH9.
[106] Sharma, A. (2018), 'Why AI Is Central to Saudi Vision 2030', AMEinfo, 14 February 2018, https://www.ameinfo.com/industry/technology/ai-central-saudi-vision-2030; Economist (2018), 'Saudi Arabia Plans for an AI Future', Economist Intelligence Unit, 27 July 2018, https://perma.cc/4LMS-U5J7.
[107] Shires, J. (2019), 'Artificial Intelligence and Security in the Gulf', in *Artificial Intelligence in the Gulf*, Gulf Research Meeting, Cambridge, UK: GRM.

both intra-GCC and regarding Iran, especially as the latter already seeks to circumvent US sanctions through cyberespionage, and tensions between Iran and the US increase?

These questions are essential for understanding not just the current state of cyber resilience in the GCC, but its future trajectory in the coming decades. Consequently, GCC governments should examine the impact of relevant new technologies on cyber resilience, discussing openly the risks of these technologies and appropriate solutions.

Conclusion

This paper has provided a necessarily high-level view across the GCC, given the large scope of the cyber resilience question. Nonetheless, this analysis suggests that there are both positive conclusions to be drawn and further challenges in improving cyber resilience in the region. On the positive side, the GCC states have invested significantly in cybersecurity and have made large strides in protecting governments, businesses and individuals from cyberthreats. It is essential to keep this momentum if ambitious national strategies, heavily dependent on advanced digital technologies, are to deliver the future visions of GCC leaders and their populations. However, the uneven nature of cybersecurity protections, and shallow implementation of cybersecurity strategies and regulations, means that GCC states need to focus on the more difficult task of cyber resilience in addition to the simpler initial stages of cybersecurity capacity-building.

In addition to increasing cyber resilience overall, there is an additional challenge in striking the right balance between different approaches to cyber resilience, related to the different threats that states face in cyberspace. The GCC states have centralized their laws, government organizations and private-sector partnerships to respond strategically to information threats, including through extensive monitoring and censorship of social media, as well as targeted responses to dissidents. This centralization means that GCC states are less able to respond to critical infrastructure attacks or financial threats, as only limited resources can be allocated between the two types of threats. A sustainable approach to cyber resilience would rebalance their priorities away from social media towards more distributed strategies, providing different elements of their economies and societies the correct incentives to protect themselves.

We have three specific recommendations that help implement this suggestion. First, GCC states could work more closely in international forums aimed at cooperation on cybercrime or capacity-building in cybersecurity or both such as the Budapest Convention on Cybercrime, the Europol Cybercrime Centre, or the Global Forum on Cyber Expertise among others. Rather than detachment from international partners, these states could look to learn and share experiences internationally. Second, differences between the GCC are crucial, as uncoordinated resilience strategies could entrench vulnerabilities in a climate of political division. GCC states should therefore prioritize cooperation across borders and within the GCC organization itself. Finally, GCC countries should anticipate and prepare for the risks posed by new technologies, including 5G, IoT and AI, as these will be an essential aspect of future cyber resilience. These risks stem from both hasty societal adoption and the role these technologies play in broader geopolitical changes.

In sum, a comprehensive approach to cyber resilience distinguishes between different threats and identifies the advantages and disadvantages of different resilience strategies in response to those threats. In the GCC, this approach has the potential to preserve and amplify the momentous gains of the digital revolution to achieve a more prosperous and fulfilling future for all those within and connected to the region.

About the Authors

James Shires is an assistant professor at the Institute for Security and Global Affairs, University of Leiden, and a non-resident research fellow with the Cyber Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School. He is also a research affiliate with the Centre for Technology and Global Affairs at the Department of Politics and International Relations, University of Oxford. His research examines cybersecurity in the Middle East and the development of cybersecurity expertise.

Joyce Hakmeh is a senior research fellow in the International Security Programme at Chatham House, and co-editor of the Journal of Cyber Policy. She specializes in cyber policy and provides regular analysis on issues that sit at the nexus between technology and geopolitics. She is developing a series of cyber capacity-building projects, including cyber simulation exercises aimed at senior decision-makers around the world. She is the co-chair of the Global Forum on Cyber Expertise (GFCE) Working Group on Cybercrime and a member of its Advisory Board.

Acknowledgments

Thanks are due to all the reviewers who contributed to this paper, including the external reviewers. This research paper is part of a three-year project, run by Chatham House and supported by the Ministry of Foreign Affairs of the Netherlands and the UK Cabinet Office, aiming to deepen the understanding of the dynamics of political and economic change in the Gulf and Arabian Peninsula.

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder. Please direct all enquiries to the publishers.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Copyright © The Royal Institute of International Affairs, 2020

Cover image: Saudi nationals attend the Gitex 2018 exhibition at the Dubai World Trade Center in Dubai on 16 October 2018.
Photo credit: Copyright © Karim Sahib/AFP/Getty

ISBN 978 1 78413 388 7

This publication is printed on FSC-certified paper.

FSC

Typeset by Soapbox, www.soapbox.co.uk