COVID-19 and the Cyber Challenge

General (Ret.) Keith B. Alexander
Jamil N. Jaffer

EXECUTIVE SUMMARY

Over the past year, a massive public health crisis has gripped the world, fundamentally changing the way individuals and entities work and interact with one another. This global pandemic has also caused new cyber threats to surface, along with the expansion of existing threats from criminal organizations and nation-states as well. This introductory piece sets out some of the key threat vectors in the cyber domain specific to COVID-19 that have emerged in the past year. It also highlights some potential paths forward to mitigate the risk presented in this new environment, including implementing critically important public-private collaboration to mitigate threats going forward.

THE VIRUS

In late December 2019, the World Health Organization (WHO) noted initial media statements emanating from China's Wuhan Province about "viral pneumonia" cases.[1] Within weeks, researchers determined these cases were cause by a novel, rapidly spreading, and life-threatening coronavirus. Nations began assessing how they might protect their populations, with many instituting travel bans and the like, but the spread of the disease proved significantly hard to control,[2] particularly given the globalized economic environment and the existence of rapid, long-distance travel. On March 11, 2020, the WHO determined that the spread and severity of COVID-19 had reached pandemic levels,[3] and by early 2021, the virus had infected over 140 million individuals and killed over 3 million worldwide.[4] With vaccines now approved and in distribution,[5] some degree of relief appears on the horizon. Much depends however, among other things, on vaccine efficacy—particularly against new virus strains—and optimal vaccine distribution.

GEN (USA, Ret) Keith B. Alexander, former director of the National Security Agency and founding commander of U.S. Cyber Command, now serves as chairman, president, and co-CEO of IronNet Cybersecurity, a start-up technology company focused on securing public and private networks and systems from major cyber threats. He also serves on the Advisory Board of the National Security Institute at George Mason University's Antonin Scalia Law School.

The COVID-19-Driven Cyber Threat Environment

The COVID-19 pandemic, while principally a public health crisis, also hugely impacts how people work and interact with those around them. In parallel with these changes to the work and social environments of the global populace, we have seen a significant increase in cyber threats across the spectrum. For example, in August 2020, INTERPOL reported a major increase in cybercrime, with the INTERPOL Secretary General starkly warning that cybercriminals were developing new attacks at an "alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."[6] The range of issues raised by the INTERPOL report includes potential threats from: (1) online scams and phishing attempts, with criminals posing as government and health authorities, looking to leverage concerns about and interest in the COVID pandemic in two-thirds of INTERPOL member countries; (2) disruptive malware, including ransomware and distributed denial of service attacks, targeting healthcare institutions and other critical infrastructure; (3) data harvesting malware used to obtain information, compromise systems and networks, extract data, and steal money; (4) malicious domains under COVID-related keywords to support criminal activities, with INTERPOL receiving nearly 600% increase in reported malicious domain registrations in a two-month period early in the coronavirus outbreak; and (5) a significant increase in misinformation and disinformation activities designed to raise anxiety, cause internal discord, and, in some cases, facilitate cyber-attacks.[7] INTERPOL reports in late 2020 also highlighted organized crime efforts to target vaccine storage facilities and distribution networks, with the INTERPOL Secretary General referring to vaccines as "liquid gold," as well as exploitation of the COVID-19 pandemic by terrorist groups seeking to "reinforce their power and influence, particularly among local populations, or to expand their external financial resources."[8]

Jamil N. Jaffer, former chief counsel and senior advisor to the Senate Foreign Relations Committee who also served in senior national security roles in the Bush Justice Department and the White House, now serves as senior vice president for strategy, partnerships, and corporate development at IronNet Cybersecurity. He also serves as founder and executive director of the National Security Institute and is an Assistant Professor of Law at George Mason University's Antonin Scalia Law School.

One key change we have seen around the globe is that, where possible, companies, government agencies, and other organizations have largely pivoted to a remote work environment.[9] One May 2020 estimate indicates that some 300 million globally now work from home.[10] Moreover, while many organizations will return to a traditional working environment due to need or preference, employers and employees increasingly anticipate that many organizations will remain in a hybrid remote work posture going forward, with significantly more employee flexibility.[11] This new work environment opens up potential new threat vectors in the cyber domain, as organizations adapt security practices to fit this new environment and extend their perimeter and other cyber defenses to home networks by using virtual private networks (VPNs) and other mechanisms. These systems are important to protect corporate content, but they can also expose a key route of access into corporate systems that attackers may be able to compromise.[12]

In the US, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) highlighted various cyber-related scams and threats seeking to exploit the COVID-19 pandemic and the new work environment. In mid-April 2020, the Secret Service and FBI jointly issued a warning that "the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before," warning that "[t]he speed at which criminals are devising and executing their schemes is truly breathtaking" and noting that the "sheer variety of frauds already uncovered is itself shocking."[13] These agencies also highlighted pandemic-related cyber fraud "targeting websites and mobile apps designed to track the spread of COVID-19 and using them to implant malware to steal financial and personal data," threat actors "posing as national and global health authorities…to conduct phishing campaigns… designed to trick recipients…into downloading malicious code," and major efforts to deploy code exposing vulnerable individuals and businesses to ransomware.[14]

At the same time, cybersecurity companies had already begun reporting large increases in ransomware attacks, up nearly 150% between February and March 2020 alone.[15] Moreover, in April 2020, CISA and the UK's National Cyber Security Centre (NCSC) issued an alert flagging a key increase in the number of financial attacks by malicious cyber actors exploiting the COVID-19 pandemic.[16] Specifically, CISA and NCSC noted that SMS and email phishing campaigns, including campaigns designed to deploy malware, were exploiting interest in the coronavirus pandemic.[17] CISA and NCSC also highlighted increased efforts to take advantage of the new work-from-home environment, with threat actors exploiting publicly known vulnerabilities in remote access software including Citrix and Microsoft RDP.[18] The FBI likewise highlighted threats to business, including those arising out of the use of telework applications, such as remote desktop software, video conferencing, and Voice over Internet Protocol (VoIP) conference call systems, as well as potential supply chain threats stemming from computer rentals from foreign sources and an increase in Business Email Compromise (BEC) scams.[19] In the same month, Google reported 18 million daily COVID-related malware and phishing emails, and more than 240 million COVID-related daily spam messages.[20] Furthermore, in June 2020, FBI leadership testified before the Senate Judiciary Committee, reporting that the use of virtual assets and encrypted devices to launder stolen money as part of COVID-19 scams made it "increasingly difficult to track illicit finance flows and identify the criminal actors behind them."[21] They also noted a significant uptick in "virtual asset fraud schemes related to COVID-19, including blackmail attempts, work-from-home scams, paying for non-existent treatments/equipment, and investment scams."[22]

These trends have continued and expanded over the course of the pandemic, taking on a more nation-state-oriented focus. In May 2020, the FBI and CISA highlighted the potential threat to US organizations conducting COVID-19-related research from Chinese cyber actors, including efforts to obtain intellectual property (IP) and data related to vaccines, treatments, and testing.[23] In late July 2020, the Justice Department announced charges against two Chinese hackers working for themselves and the Chinese Ministry of State Security (MSS), targeting companies, governments, non-governmental organizations, and individuals, stealing terabytes of data by targeting computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.[24] In May 2020, CISA and the UK's NCSC confirmed investigations of advanced persistent threat (APT) activity targeting healthcare and essential services, including pharmaceutical companies, universities, medical research organizations, and local governments, in part to obtain information on COVID-19-related research efforts.[25] These actors were using techniques including password spraying and scanning targets for unpatched vulnerabilities, including those in Citrix software and VPN products from Pulse Secure, Fortinet, and Palo Alto, many of the systems also used to enable and protect the new at-home workforce.[26] CISA and NCSC further noted significantly increased risk to international business supply chains because APT actors saw these supply chains as weak links, potentially enabling access to otherwise well-protected targets.[27]

Likewise, the international financial system faces significant operational risks from well-resourced nation-state and key non-nation-state attackers, as remote work increasingly forces banks to identify and onboard new customers online and as regulatory bodies provide relief on typical anti-money laundering requirements.[28] These risks are rendered even more serious because they arise in the context of a strong ongoing effort by the US and other governments worldwide to inject capital into their national and regional economies.[29] Specifically, given the new pandemic environment, key international financial organizations assess that it is increasingly likely that online financial services will be used for money laundering, and that there is a major and growing risk of corruption and misuse of government stimulus funds and international financial aid.[30]

Of course, we have also seen increased misinformation and disinformation by nation-states during the pandemic, whether to blame the US for the coronavirus, as in the case of China, Russia, and Iran,[31] or to suggest that authoritarian governments may have an edge in fighting such diseases.[32] All of these threats, taken together, demonstrate that the global geopolitical environment, particularly in cyberspace, is getting more dangerous as the pandemic continues forward.

Managing the Nation-State Cyber Threat During the COVID Epidemic

Given all this, key questions that authors in this special edition of *The Cyber Defense Review* will grapple include identifying and stopping cyber threats enabled by this global pandemic, addressing pandemic-related social media exploitation by nation-states, and ensuring government and industry continuity of operations. This edition's authors analyze these cyber risks with all the usual key policy and public issues in play, including data privacy, surveillance, the exploitation of public fears by adversarial nation-states, anxiety, existing social upheaval, national security, increased geopolitical risks, and ensuring appropriate national and international preparedness and resilience. Indeed, one of the key themes that surfaces across the various articles in this volume is the criticality of building strong and sustainable operational relationships within and across the public and private sectors and across international boundaries.

For far too long, the cybersecurity policy community has accepted as given the idea that organizations, both in the government and private sector, should each be primarily responsible for their own defense, whether against run-of-the-mill cyber adversaries or nation-state advanced persistent threats. However, as we argued in these pages nearly four years ago, if the goal is to create a truly defensible national (or international) cyber architecture, this approach makes little sense, at least against nation-state-level threat actors.[33] The pandemic further highlights this challenge. Whether one discusses the threat to the vaccine development and distribution infrastructure posed by Chinese or Russian nation-state cyber actors, or nation-state efforts to undermine public confidence in private sector entities developing these capabilities, and regardless of whether such efforts are aimed at national political or economic goals, neither private nor public sector entities standing alone can realistically be

expected to defend themselves—or this nation—against nation-state-level threat actors in the cyber domain. Even the most capable of these entities—large financial sector organizations that have long faced significant, sustained cyber-attacks from a wide range of threat actors and which recognize such attacks as presenting "the biggest threat to the US financial system"[34]—remain vulnerable when it comes to defending effectively. And, as noted above, such organizations have been a priority focus of nation-state and other key threat actors throughout the COVID-19 pandemic.[35]

It is not just us nor the authors in this volume who have identified this serious challenge. Indeed, the Cyberspace Solarium Commission highlighted this same issue in its March 2020 report, in which the commissioners unanimously called for the public and private sectors to "arrive at a new social contract of shared responsibility to secure the nation in cyberspace."[36] As the Commission put it, creating true "collective defense in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverage its unique comparative advantages for the common defense."[37] Likewise, other authors in this journal recently highlighted the critical importance of public-private partnerships and collaboration noted in the Commission's report.[38] Moreover, as the pandemic has all too well highlighted, recent years have seen a fundamental shift in the cyber threat landscape, as attackers who once focused on government national security agencies are now pivoting to private sector companies and government institutions farther down the spectrum. The recently disclosed SOLARSTORM hack and associated efforts by the Russian SVR reflect this pivot as do the HAFNIUM hacks conducted against the Microsoft Exchange infrastructure by Chinese actors.[39] Indeed, this particular hack's targeting of national security and civilian government agencies and key private sector entities in the supply chain highlights the expanding scope and nature of the current threat.

The pandemic, SOLARSTORM, and HAFNIUM hacks have also illuminated the huge mismatch between threats and defenses in the modern cyber environment that can no longer go unaddressed. We can no longer expect individual companies—driven principally by the need to deliver products and services to consumers or other organizations—nor individual government agencies or states and localities—focused on their own constituencies—to stand alone against the threat posed by nation-state attackers who have access to virtually unlimited human, economic, and technical resources.[40] Nor can we continue to expect key allies in regions threatened by overaggressive cyber actors—whether Chinese, Russians, Iranians, or North Koreans—to stand alone against these threats.[41] Consistent with Cyberspace Solarium Commission recommendations, we must enhance the US ability to create shared situational awareness in cyberspace, including creation of a joint collaborative environment in the United States,[42] as well as similar constructs with European[43] and other allies.[44] These capabilities will not only require large-scale collection and sharing of actionable cyber threat intelligence amongst the public and private sectors and with allies, but will also demand significant operational collaboration. Information sharing is but a means to an end. The ultimate

goal is truly enhanced, shared cybersecurity and the creation of a strong, sustainable defensive cyber fabric, which will require us to be highly efficient and effective in operating collectively across traditional divides.

Finally, it is important to note that the cyber threats that have surfaced in the wake of the pandemic, including the recent SOLARSTORM and HAFNIUM hacks, also underscore the vulnerability of our global supply chains, both in the physical world as well as in the cyber domain. Defending ourselves in this space effectively requires immediate action to build out and support an assured allied ecosystem for critical resources, both in technology and related industries, including innovation in cutting-edge communications capabilities, development and testing of semiconductors, mining and processing of the rare earth metals required by computing and other critical technologies, and supporting and expanding advancements in machine learning and quantum computing.[45] We must also establish a clear, declarative policy on threats to our cyber infrastructure, ensuring the world fully understands our capability and resolve to impose crippling costs, both cyber and physical, on those who would do us harm whether nation-state actors or their proxies. Such policies must apply to those that would engage in, or even threaten, cyber operations that could seriously damage, destroy, disrupt, or modify key data or systems. Our bottom line should be a clear policy: the US will protect itself—both the public and private sectors—and our allies against serious hostile actions or threats against our cyber infrastructure with no less resolve than against threats in the physical domain.

If these recommendations seem edgy or forward-leaning, our experience living through the pandemic has demonstrated that the smart approach, when we see a threat surfacing on the horizon, is to act in advance, rather than waiting for it to arrive on our shores. We can now see clearly the threat that nation-state adversaries present to our modern economy and national security; the question remains whether we finally have the resolve and fortitude to do what is necessary to meet it head on.

NOTES

1. World Health Organization, *Listings of WHO's Response to COVID-19*, June 29, 2020, http://who.int/news/item/29-06-2020-covidtimeline/.
2. Chad R. Wells, etal., *Impact of International Travel and Border Control Measures on the Global Spread of the Novel 2019 Coronavirus Outbreak*, Proceedings of the National Academies of Sciences of the United States of America (March 31, 2020), https://www.pnas.org/content/117/13/7504.
3. World Health Organization, *Listings of WHO's Response to COVID-19, supra* n. 1.
4. World Health Organization, *WHO Coronavirus Disease (COVID-19) Dashboard* (February 24, 2021), reporting 111,762,965 cases of COVID-19 worldwide and 2,479,678 deaths, https://covid19.who.int/.
5. U.S. Food and Drug Administration, COVID-19 Frequently Asked Questions, (noting that "[o]n December 11, 2020, the FDA issued an Emergency Use Authorization (EUA) for the use of the Pfizer-BioNTech COVID-19 Vaccine...[and] [o]n December 18, 2020, the FDA issued an EUA for the use of the Moderna COVID-19 Vaccine."), https://www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/covid-19-frequently-asked-questions#biologics.
6. INTERPOL, *INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19* (August 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
7. Ibid.
8. INTERPOL, *COVID-19 Crime: INTERPOL Issues New Guidelines for Law Enforcement* (November 17, 2020), https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-crime-INTERPOL-issues-new-guidelines-for-law-enforcement; INTERPOL, *INTERPOL Warns of Organized Crime Threat to COVID-19 Vaccines* (December 2, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines; INTERPOL, *INTERPOL – Terrorist Groups Using COVID-19 to Reinforce Power and Influence* (December 22, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-Terrorist-groups-using-COVID-19-to-reinforce-power-and-influence.
9. Rita Zeidner, *Coronavirus Makes Work from Home the New Normal*, Society for Human Resource Management (March 21, 2020), https://www.shrm.org/hr-today/news/all-things-work/pages/remote-work-has-become-the-new-normal.aspx.
10. Juan Carlos Crisanto and Jermy Prenio, *Financial Crime in Times of COVID-19 – AML and Cyber Resilience Measures, FSI Briefs*, No. 7 (May 2020), https://www.bis.org/fsi/fsibriefs7.pdf, 2.
11. PriceWaterhouseCoopers, *It's Time to Reimagine Where and How Work Will Get Done*, PwC's US Remote Work Survey (January 12, 2021), https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html; Brodie Boland, et al., *Reimagining the Office and Work Life after COVID-19* (June 8, 2020), McKinsey & Co., https://www.mckinsey.com/business-functions/organization/our-insights/reimagining-the-office-and-work-life-after-covid-19#.
12. National Security Agency, *Mitigating Recent VPN Vulnerabilities* (October 7, 2019), https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF; Vijay Sarvepalli, *VPN – A Gateway for Vulnerabilities*, Carnegie Mellon University: Software Engineering Institute (November 13, 2019), https://insights.sei.cmu.edu/cert/2019/11/vpn---a-gateway-for-vulnerabilities.html.
13. Federal Bureau of Investigation, *FBI and Secret Service Working Against COVID-19 Threats* (April 15, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats.
14. Ibid.
15. VMWare Carbon Black, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted* (April 15, 2020), https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.
16. Department of Homeland Security, *COVID-19 Exploited by Malicious Cyber Actors*, CISA Alert AA20-099A (April 8, 2020), https://www.us-cert.gov/ncas/alerts/aa20-099a.
17. Ibid.
18. Ibid.
19. Federal Bureau of Investigation, *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*, Alert Number I-040120-PSA (April 1, 2020), https://www.ic3.gov/Media/Y2020/PSA200401.

NOTES

20. Steven Musil, G*oogle Blocking 18M Malicious Coronavirus Emails Every Day,* CNET (April 15, 2020), https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/.
21. Calvin A. Shivers, *Statement Before the Senate Judiciary Committee: COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic* (June 9, 2020), https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic.
22. Ibid.
23. Federal Bureau of Investigation, *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations* (May 13, 2020), https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations.
24. Department of Justice, *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research* (July 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
25. Cyber and Infrastructure Security Agency, A*PT Groups Target Healthcare and Essential Services,* Alert AA20-126A (May 5, 2020), https://us-cert.cisa.gov/ncas/alerts/AA20126A.
26. Ibid.
27. Ibid.
28. Crisanto and Prenio, *Financial Crime, supra* n. 10, 2-4, 6-8.
29. Tim Maurer and Arthur Nelson, *COVID-19's Other Virus: Targeting the Financial System,* Carnegie Europe (April 21, 2020), https://carnegieeurope.eu/strategiceurope/81599.
30. Crisanto and Prenio, *Financial Crime, supra* n. 10, 2.
31. Natasha Bajema and Christine Parthemore, *How to Counter China's Coronavirus Disinformation Campaign* (March 29, 2020), *Defense One,* https://www.defenseone.com/ideas/2020/03/how-counter-chinas-covid-19-disinformation-campaign/164188/; Julian Barnes, et al., *As Virus Spreads, China and Russia See Openings for Disinformation* (March 28, 2020); T*he New York Times,* https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html; U.S. State Department, *Iran: COVID-19 Disinformation Fact Sheet* (March 23, 2020), https://www.state.gov/iran-covid-19-disinformation-fact-sheet/.
32. Will Knight, *China Flexes Its Soft Power With 'Covid Diplomacy,' Wired* (April 2, 2020), https://www.wired.com/story/china-flexes-soft-power-covid-diplomacy/.
33. Keith B. Alexander, et al, *Clear Thinking About Protecting the Nation in the Cyber Domain,* The Cyber Defense Review, Vol. 2 No. 1, 29, 33, (2017), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Clear%20Thinking%20About%20Protecting_Alexander_Jaffer_Brunet.pdf?ver=2018-07-31-093723-563.
34. Jamie Dimon, *Letter to Shareholders,* 35, JP Morgan Chase (April 2019), https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf.
35. Jamil N. Jaffer, *Prepared Statement of Jamil N. Jaffer on Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic,* Subcommittee on National Security, International Development and Monetary Policy, United States House of Representatives Committee on Financial Services (June 16, 2020), https://nationalsecurity.gmu.edu/wp-content/uploads/2020/06/Jaffer-House-Financial-Services-Subcommittee-Testimony-on-Financial-Sector-Cyber-Threats-For-Circulation-6.15.20.pdf.
36. Cyberspace Solarium Commission, *Commission Report* (March 2020), 96, https://www.solarium.gov/report.
37. Ibid.
38. Joe Reeder and Robert E. Barnsby, A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership, *The Cyber Defense Review* (Fall 2020), https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2003_Reeder_Barnsby.pdf.
39. Federal Bureau of Investigation, et al., *Joint Statement by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence, and the National Security Agency (NSA)* (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

NOTES

40. Keith B. Alexander and Jamil N. Jaffer, *The Other Crisis: U.S. Companies Still Need Help Against Cyberattacks, Barron's* (March 26, 2020), https://www.barrons.com/articles/cyberspace-solarium-commission-urges-collective-defense-51584364449.
41. Keith B. Alexander and Jamil N. Jaffer, E*nsuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition, 19 Geo. J. Int'l Aff.* 51, 52-58 (Fall 2018), http://nationalsecurity.gmu.edu/wp-content/uploads/2018/10/GJIA-19-1-FINAL-rev-57-72.pdf.
42. *Cyberspace Solarium Commission Report, supra* n. 35, 101-102.
43. Keith B. Alexander (with Jamil N. Jaffer), *A Transatlantic Alliance Is Crucial in an Era of Cyberwarfare, Financial Times* (September 4, 2018), https://www.ft.com/content/c01a7f94-af81-11e8-87e0-d84e0d934341.
44. Keith B. Alexander and Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks? The Hill* (May 15, 2019), https://thehill.com/opinion/national-security/443610-irans-coming-response-increased-terrorism-and-cyber-attacks (Middle East allies); *Ensuring U.S. Dominance, supra* n. 38, 52-58 (Asian and other allies); Jamil N. Jaffer, *U.S.-India Relations on Cybersecurity: An Important Moment for Strategic Action on Collective Cyber Defense* in *ENHANCING U.S-INDIA STRATEGIC COOPERATION* (Manchester University Press, 2021, forthcoming).
45. Keith B. Alexander and Jamil N. Jaffer, *China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around, Barron's* (August 4, 2020), https://www.barrons.com/articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400.