Civilians 'Defending Forward' in Cyberspace

Aligning cyber strategy and cyber operations

Dr. Matthew J. Flynn

ABSTRACT

Examining the 'defending forward' concept and the intersection between DoD and the private sector speaks to aligning instruments of national power to set the stage for the consolidation of Internet connectivity and an expansion of that capability. Both outcomes feed a new understanding of what a professional military does in the cyber age to safeguard a civilian interface that is revamping the norms of government across state boundaries. Implementing an effective cyber strategy necessitates recasting the US military's cyber operations to support civilian efforts. A dramatic point of departure from the current emphasis, this change in focus will prevent the US military from leading a non-violent conflict at odds with war in the corporal world. Instead, civilians will be charged with winning the fight in the cognitive arena of cyberspace.

Civilian entities have put themselves in a state of readiness in terms of cyber security that begs the question of exactly what role the US military should play in cyberspace. In several ways, private business is 'defending forward' and waging war in cyberspace, overtly at times. This effort means that the civilian sector seeks to disrupt and halt malicious cyber activity at its source, and degrades such activity before it can reach its intended victims, in parallel with the aim of the Department of Defense's (DoD) new mandate of defending forward.[1] Detecting and reporting threats from malicious online actors, revealing how those actors frequently work at the behest of nation states, and offering exploits to counter such activity are essential elements of the DoD's active preparedness in cyberspace.

This positioning also means an attempt to exceed the defense of critical resources and related sectors of the economy to engage in a messaging war that accompanies technical attacks and threats in cyberspace. Yet, the private sector already engages in an online information offensive, and in so doing counters the potential of an inimical US military presence in cyberspace looking to police thoughts exchanged on the Internet. Recognition of the private sector's needed ability to check military largess in this capacity is only slowly coming into focus, but may well constitute the most important measure of the defending forward strategy.

This article calls for the US military to accept the civilian defense of an open Internet that is critical to the success of the future of cyberspace. Leveraging the status quo of "openness" centers attention on the Clausewitzian contest of wills in order to pursue a change in mindset more than a correction in behavior assumed to accompany an act of military force. Defending forward in cyberspace with civilians in the lead can achieve a lasting impact via an act of coercion that seeks a cognitive end, less a physical measure. That intellectual application of war, the most essential measure of a contest of wills, is well-suited to the ether of cyberspace.

In providing a service facilitating a population's access to the Internet and doing so without government oversight, the private sector has delivered the most important function of openness. Whether by balloons, drones, or satellites, these companies provide connectivity to some three billion people and now look to connect the rest of humanity, a further five billion people. This goal may prove overly ambitious, but it means that the number of people online will continue to rise. Even assigning the self-interested motive of gaining market share to those businesses so engaged does little to forestall the reality that with more people online, connectivity remains a powerful reality and so too openness.

A society welcoming openness clashes with authoritarian regimes that recoil before the universal right of users to uncensored information and privacy inherent in a globally connected world. In this democratic purpose lies the intellectual battlefield of cyberspace. Yet, leaders in technology advance openness seemingly oblivious to the ideological implications of what they are advocating. Mark Zuckerberg, CEO of Facebook, proudly issued a call to connect the world when he stood before the United Nations (UN) in September 2015 and identified greater connectivity as "one of the fundamental challenges of our generation." Bringing online access to a further four billion people will empower humanity economically and even socially, he argued. Zuckerberg's UN declaration advanced Facebook's policy from the year before.[2] In taking this stand, there is no recognition of the cyber ideology embedded in openness that underscores the political ramifications of being online, or the potential for pushback from states threatened by ever broadening Internet access.

The inconsistency of those in the private sector who advance a natural progression towards online interaction, all the while refusing to acknowledge that connectivity invites political plurality, allows government officials to pursue cyber sovereignty. But trying to apply territorial restrictions to cyberspace invites unwarranted military action to curb public expression to

enforce borders in the domain. That effort heightens threats of war that, if acted on, could cripple openness. The risk looms large enough to prompt Microsoft president and chief legal officer Brad Smith to openly appeal for a Digital Geneva Convention in order to prevent cyber conflict that threatens civilian access to a global Internet. In early 2017, he warned an audience at the RSA conference on IT security in San Francisco that the perversion of the medium is at stake and that a cyber war could undo the universal norms of the platform. While governments have a long history of negotiating and observing international rules to restrict the impact of military actions against civilians, Smith argued that business should lead a call on behalf of safeguarding cyberspace.[3] That a private entity co-opted treaty norms restricting military actions underscores the urgency of business to take the lead in defending openness, thereby, albeit unintentionally, taking the lead in defending forward.

Any brokering of peace in cyberspace will require recognition and, to some extent, legitimation of the ideological struggle in that domain that comes with openness. Despite the absence of international conventions or other agreements to call out this distinction, ideological battles over openness are already underway, with civilians in the lead. The civilian-led fight—no matter how unwittingly—ranges from more or less innocuous websites verbally supporting activist movements to websites offering activists tools for defying online censorship by the outright unblocking of Internet traffic. These services include a VPN offensive targeting specific nations that look to restrict the online communications of their citizens. The progression of a means to promote openness moves from providing a service, to enabling defiance, to direct attack that, when taken together, reflect the capacity of the private sector to defend forward in cyberspace.

Organizations that offer platforms that provide openness as a common good instill hope among online users who might otherwise despair. A number of global citizen networks provide this form of service. For example, the Thai Netizen Network, founded in December 2008, advocates for civil rights and democracy online.[4] That body upholds the broadest tenets of openness in the face of a strong reactionary movement in Thailand. In February 2019, the Thai government passed a cybersecurity bill creating a government agency to restrict Internet access in the name of countering cyber threats. The National Cybersecurity Committee, answerable to the prime minister, can now use the broad language of the law to ensure the regulating authority of the state to enforce standards and restrictions on Internet access that accord with government concerns that touch every aspect of online use. In short, in a government dominated by a military presence, authoritarianism took a huge step forward in heading off public dissent by enforcing cyber security laws, but global citizen networks, as civilian entities, can circumvent these limits.

Other nations in the Southeast Asian region took similar steps to curb supposed abuses inherent in the cyber medium to make it "safe" for users by thwarting access to information. Vietnam passed a “Cyber Security Law” effective January 1, 2019. In very clear language, the law curtails openness online. One provision of the law, Article 16, prevents “propaganda”

against the state, banning "information contents which incite riots, disrupt security or cause public disorder, which cause embarrassment or are slanderous, or which violate economic management order."[5] In Indonesia in January 2018, President Joko Widodo appointed Major General Djoko Setiadi as chief of the country's new National Cyber Encryption Agency (BSSN), an agency that operates under direct presidential control. This "cyber command" targets fake news, crime, and online extremists. It also sparks fears of eroding civil liberties. By the end of 2018, Indonesia's legislature started to weigh the merits of a cyber security bill. That effort is pending.[6]

In many ways, these nations are following the lead of China. That nation's "Internet Security Law" became effective on June 1, 2017. The government carefully targeted the law to silence online voices that might spur or coordinate civilian activism. Article 12 demands that users "...must not use the internet to engage in activities endangering national...interests; they must not incite subversion of national sovereignty, overturn the socialist system...or disseminate false information to disrupt the economic or social order... ."[7] This sweeping indictment of Internet functionality also underscores the platform's capacity for enabling political activism and the regime's vulnerability to the mere act of connectivity. Openness triggers this counter move from closed regimes, a tension that plays out across Southeast Asia and the Pacific as the region's power centers employ cyber security measures to target openness as inimical to state interests, challenging the democratic process.

In response to state repression comes a civilian online response. The Asia Internet Coalition seeks "to promote the understanding and resolution of Internet policy issues in the Asia Pacific region."[8] Its members include Google, Facebook, Amazon, Twitter, and Apple. This consortium exerts obvious international financial clout. With that standing and, therefore, influence, comes the latent threat of demanding online access for all users, free of oversight, since oversight complicates business practices. Far from a union of state and commercial interests, the coalition stands in defiance of any government seeking to limit user access to maintain control.

Business appears ready to take things even further as the tech industry improves encryption protection to curtail eavesdropping by government on Internet communications. Many companies can scramble information so it can pass data onto an end user without its content being discerned. At the same time, many other companies promise decoding of encrypted communication to forestall potential threats to networks from malware and unwanted intrusion or messaging. In offering a fix, these companies promise relief from increasing cyber threats and offer beleaguered governments a chance to find their footing. Worse, many powerful tech companies have bowed to the demands of overtly authoritarian governments to tailor their interfaces to prevent the user from enjoying unfettered online access. In the case of Facebook, the company has argued that a limited inroad is better than no inroad at all.[9] This give and take illustrates the clash of values between the cyber self-determination of users and the control of access by self-declared cyber-authorities online. The cyber domain is at once an open space inviting free and unconstrained human interaction but as such it also draws attempts at governmental

control of that very impulse. That duality of cyberspace remains simply too threatening for most societies to leave unpoliced. That tension puts the tech industry at the heart of brokering the means of governance at the expense of government, a tension that has placed defending forward in the hands of civilians.

Parts of the world other than Asia also face similar online challenges. European nations began to test legal measures featuring government oversight of Internet openness to thwart online disinformation. This counter to Russian attempts to influence European elections was a move toward censorship via tighter government controls. Having just endured such meddling in its 2017 presidential election, in July 2018, the French National Assembly drafted two laws to prohibit the manipulation of information online. The proposed changes to the Electoral Code required social media companies to alert users to false information and allowed a judge forty-eight hours to declare the content harmful and to be removed. This mechanism would be enforced three months prior to a national election. Citing the difficulty of making such a determination in a short timeframe, the French Senate rejected the measure at the end of 2018.[10] The year before, a similar law in Germany survived the two chambers of the legislature. Germany's Network Enforcement Act became effective on October 1, 2017. The so-called "Facebook Act" looked to combat hate speech and fake news posted on social media by demanding social media outlets remove material deemed "unlawful" within 24 hours of notification, or face large fines.[11] The difficulty of determining what was harmful and therefore unlawful went unchallenged.

In confronting the fear of manipulated information, European nations were striving to preserve their democratic ideals, but felt the same temptation to sacrifice freedom for order and safety as plagued Asia. Fortunately, civilian organizations arose and took on the challenge of documenting online attacks on truth. In 2015, the European Union (EU) created a task force to document examples of pro-Kremlin disinformation carried in the media. The EU vs. Disinfo website publishes a "review" of such abuses, all pursued and substantiated by civilian activists. The webpage offers an indictment of those propagating misinformation, a charge that grows stronger with the passage of time and the growing accumulation of falsehoods.[12] Ukrainians established "Stop Fake," a fact checking site designed by journalists, students, and IT specialists to rebut fake information about Ukraine and EU states.[13] This accountability movement modeled a path that avoided censorship via government controls or public vigilantes, advocating as their call to arms that the population become better informed via websites. The Stop Fake model leverages democracy's strongest attributes, its citizens, and moves society away from allowing government agencies to police information and open communication. The EU took this logic a step further when guaranteeing user control of personal data with the General Data Protection Regulation (GDPR) directive of May 2018. By demanding company accountability in the digital sphere on behalf of consumers, the EU struck a delicate balance between government oversight and free enterprise. By looking to empower citizens, a step toward tyranny has been averted.

Russia did not resist that temptation. President Vladimir Putin hoped to cement state online control via laws designed to ensure government authority over all Internet communication. That legislative wall suffers from many cracks, however. For instance, news outlets reported that some 15,000 protesters gathered in Moscow on Sunday, March 17, 2019, after Parliament advanced a digital sovereignty bill creating a government center for monitoring and controlling public communication networks.[14] The Russia effort to restrict Internet access amounts to censorship in the name of national security much as did Soviet decrees trying to shape culture via government ordinance. Neither effort worked in practice. The same goal to control drove the recent law that merely capped a long-pursued effort to reign in the Internet, allowing Russian government officials to punish individuals with fines or jail time for publishing "unreliable" information online that "disrespects" the state and society. Public statements from Russian officials asserted that the government merely needed to crack down on fake news, much as political figures in western states declare they need to do.[15] The impracticality of such state supervision means that the cyber frontier stands ready to welcome Russian activists, if not in the name of democracy, then in the name of governance surpassing barriers to achieve a cognitive freedom. The attempt at control primarily expresses the worry of authoritarian leaders in the face of practical limits on curbing public activism and dissent online.

The civilian response enjoys support from a systematic effort among online organizations willing to engage the issue of how best to protect access to information. The veiled threat coming from users sharing networks and making openness real yields to those determined to deliver on that promise. An entire industry of skilled IT professionals supports those calling for connectivity. Access now, for instance, declares its mission as preventing Internet shutdowns. By outing violators and those looking to sabotage the Internet, this organization "fights shutdowns around the world." This body also publishes a statement of ideals defending openness with the observation that, "The Internet enables all our human rights, and we need our leaders to pledge to #KeepItOn."[16] Another example highlights the actions of NGOs. AGORA International, a group of lawyers advocating for human rights, denounced Russia's efforts to restrict Internet access in a document titled, "Russia. Internet Freedom 2016: On a War Footing."[17] While what constitutes a war footing goes conspicuously undefined, the efforts of the Russian government to stymie online access is documented in alarming detail. Putin's war against sharing information is moved from secret and invisible to shamefully clear.

The escalation from innocuous pronouncements to relatively more aggressive declarations soon gives way to providing tools for direct assaults on those curbing online freedom. The VPN war on closed states continues. China remains a target and a host of companies offer access to the Chinese people without PRC approval, thereby purporting the message of openness. For example, GreatFire.org, an anonymous organization based in China, claims to "monitor and challenge internet censorship in China."[18] It offers web applications to do just that, including a browser that delivers uncensored news, electronic access to banned books, and re-published

censored information from WeChat and Weibo, China's most popular social media applications. Tech experts have also turned their attention to Russia. A number of services such as CYBERGHOST connect users to Telegram, the VPN in Russia that evades and defies government control. A website called VPNMENTOR lists the many VPNs that do the same thing in Iran and China as well as Russia i.e. enabling Telegram and making that VPN a means of communication for users seeking a voice in authoritarian states.[19] Other organizations seek to expand this offensive beyond merely VPN service. LANTERN is a US-government-funded open-source proxy service developed by Brave New Software and initiated in 2013, that looks to "bypass internet censorship and firewalls" to "secure access to an open internet." DEFLECT is a website security service that protects its clients, such as those sponsoring the *Black Lives Matter* website, from distributed denial of service (DDoS) attacks and in that way defends "civil society and human rights groups from digital attack."[20]

VPN services and related technology receive avid endorsement from the business community. The Open Technology Fund (OTF) provides financial assistance to those engaged in that endeavor. OTF declares its purpose in the familiar language of optimism about humanity's reach for openness. An OTF statement lays out the problem: "The communication of people in more than 60 countries around the world are regularly censored, surveilled, and blocked." To stop these practices, the fund will "support technology-centric solutions." In this way, the organization defies those states that "deny millions of people access to a democratic way of life and positive social change."[21] Advocating for this fundamental human right joins the ideological struggle over connectivity in cyberspace.

The business alliance continues apace. The Cybersecurity Tech Accord "promotes a safer online world by fostering collaboration among global technology companies... ." That purpose rests on four shared values among all signatories: a strong defense, no offensive actions, capacity building, and collective response. Common purpose will bind the online world together through broad use of these best practices featuring collaboration that hardens defenses to frustrate exploitation of vulnerabilities, a step fundamental to improving the reliability of products and services. Still, the concept of better security via shared commitments to cooperation across the "wider global technology ecosystem" is a familiar notion to those accustomed to the language of conflict deterrence. Emphasizing defense, discouraging attack, and building alliances mirrors the logic of diplomatic and military agreements among states. However, in the context of Internet access, this deterrence effort binds over 100 companies "committed to protecting cyberspace," including familiar powerhouses in cyber technology such as Microsoft, Intuit, CISCO, and Facebook.[22]

That language paralleling a military footing is intentional, as Microsoft President Brad Smith made explicit when he spoke at the RSA Web Summit in Lisbon, Portugal, in November 2018. In his address, Smith went to great lengths to demand that the technology industry assert itself in the ongoing cyber war. He said, "Like it or not...the reality is nonetheless inescapable. We

have become the battlefield."[23] That declaration accepted defending forward as the de facto truth, a mandate staring the business community in the face and requiring a response. That response could only take one form: the tech community waging the cyber war by recognizing its ability to compel states to resolve their differences by means short of military action.

The business community surpassing the US military in terms of defending forward in cyberspace points to the latter's slow recognition of the strategic advantage stemming from openness—an ideological offensive resting on technological development that both continues the quest for universal online access and arrests a military push to secure cyberspace on behalf of government that threatens that very pursuit. Greater clarity means the conversation on cyber policy should turn away from the reflexive impulse to 'strike back' to support preserving openness. Since advancing an open, secure, stable, accessible and peaceful cyberspace is US cyber policy, and it largely goes unrecognized, something must be done to make clear that this stand is sound policy, and one predicated on a whole of government response.[24] This need means maintaining a preponderance of US military power with a global reach to limit violent conflicts that threaten to escalate. It also means that after delivering this deterrence, the US military has a limited role to play in cyberspace. Here, defending openness requires efforts to blunt the call for cyber sovereignty and instead broker international agreements to protect a global commons, ensure government allegiance with private industry to shore-up the credibility of social media, and foster government support of the private sector advancing openness as a universal human right in cyberspace. That ideological campaign already stands at the heart of US cyber policy. In short, little has to change other than that US cyber policy must be recognized and accepted as sound policy among its critics.

In failing to grasp this pivot, the United States cedes the defense of Internet openness to the international community. France hosted a "Paris Call" for building "trust and security in cyberspace" on November 12, 2018. While the United States failed to attend, sixty-five states, 138 civil society organizations, and 344 entities of the private sector did attend, reaffirming the decree to uphold "an open, secure, stable, accessible and peaceful cyberspace."[25] The US government's absence accentuated the new militarism unfolding in cyberspace thanks to the effort of the private sector, an effort demanding cognitive struggle as a norm and something unfolding without violence as a means of settlement. This mandate informs a US cyber policy that now rests in the hands of the US military charged with striking back in cyberspace via defending forward. That strategy undermines the effectiveness of the civilian mission of defending forward by imposing one's will on an adversary with the ideological war for openness. Instead, in the US model, nonviolent actions are military acts by military actors. This incongruity represents a clear point of departure from other states organizing to wage the cyber war as a mission of peace-minded, private organizations looking to hold states in check in cyberspace.

The Paris meeting built upon some very specific and pointed antecedents. Previous, tentative calls for a cyber treaty had unfolded to manage the developing crisis in cyberspace. The efforts foundered, unsurprisingly, overcome by the impossibility of appropriating the existing norms and constructs of international relations. Borders, alliances, monitoring verifiable arms and, most significantly, recognizing a threat to one's vitality, all faced obfuscation in cyberspace when government became the agent of control. Governance proves the larger and more meaningful arbiter of international norms, no matter its apparent unwieldiness. Civilians have grasped this new reality and the need to get beyond an embrace of war terminology in pursuit of nation-state security in the new age. The call for online access as an endorsement of freedom of expression and openness means recapturing the inspirational appeal of those seeking to excel at technological prowess. In that light, defending forward becomes the foremost quest in cyberspace thanks to a civilian body embracing its call to champion conflict that unfolds in that cognitive sphere without the traditional trappings of physical conflict as war which has accumulated centuries of authority. The US military would do well to ensure its cyber operations support this larger strategic focus.

Author Bio

Dr. Matthew J. Flynn

Matthew J. Flynn, PhD., is Professor of War Studies at Marine Corps University, Quantico VA. He specializes in the evolution of warfare and has written on topics such as preemptive war, revolutionary war, borders and frontiers, and militarization in the cyber domain.

NOTES

1. For the formal articulation of defending forward as reaching beyond DOD networks and countering adversaries in the era of persistent engagement, see "Summary: Department of Defense Cyber Strategy," DOD, 2018: 1, 4; and "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," April 2018: 4, 6.
2. "Facebook CEO Mark Zuckerberg at the UN," September 26, 2015, http://www.un.org/pga/70/2015/09/26/facebook-ceo-mark-zuckerberg-at-the-un/, accessed September 27, 2015. See Mark Zuckerberg announcing that Internet.org will seek to make "basic internet services available to every person in the world." Mark Zuckerberg, Facebook, March 27, 2014, https://www.facebook.com/zuck/posts/10101322049893211, accessed April 26, 2015. See Facebook's goal of connecting "the next 5 billion people" in, "Is Connectivity a Human Right?" an undated 10-page document at the following address: https://www.facebook.com/isconnectivityahumanright, accessed April 26, 2015.
3. Brad Smith, RSA Conference, "The Need for a Digital Geneva Convention," February 14, 2017, San Francisco, California: https://www.youtube.com/watch?v=C-YvpuJO6pQ, accessed May 8, 2019. And, "The Need for a Digital Geneva Convention," Brad Smith, Microsoft, Blog Post, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001f0wujpo0tdrhytq2edlwmgn9i, accessed May 15, 2019. See also Microsoft Policy Paper, "A Digital Convention to Protect Cyberspace," no date.
4. Thai Netizen Network, https://thainetizen.org/about, accessed July 8, 2019.
5. "Law 24 on Cybersecurity, dated June 12, 2018," Chapter 3, Prevention of and Dealing with an Infringement of Cybersecurity, Article 16, page 11, from Vietnam Laws Online Database, Allens International Law Firm, www.vietnamlaws.com, accessed July 8, 2019.
6. "Indonesia's New Cyber Agency Looks to Recruit Staff of Hundreds," Kanupriya Kapoor, *Reuters*, January 5, 2018. See reference to, "Bill on Security and Security of Cyber," National Legislation Program, Board of People's Representatives of the Republic of Indonesia, www.dpr.goid/prolegnas/index/id/223#, accessed July 8, 2019.
7. Article 12, "Cybersecurity Law of the People's Republic of China (Second Draft)," translation by the American Chamber of Commerce - China, no date.
8. Asia Internet Coalition, "About," https://aicasia.org/about/, accessed July 8, 2019.
9. Mark Zuckerberg, Facebook Post on March 16, 2015, https://www.facebook.com/zuck/posts/10101974380267911, accessed March 17, 2015.
10. "Senate Rejects 'Fake News Ban' Bills," September 24, 2018, Global Legal Monitor, The Law Library of Congress, www.loc.gov/law/foreign-news/article/france-senate-rejects-fake-news-ban-bills/, accessed July 9, 2019.
11. "Social Media Platforms to be Held Accountable for Hosted Content under 'Facebook act,'" July 11, 2017, Global Legal Monitor, The Law Library of Congress, www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountalbe-for-hosted-content-under-facebook-act/, accessed July 9, 2019.
12. EU vs Disinfo, "About," https://euvsdisinfo.eu/about, accessed July 9, 2019.
13. Stop Fake, "About," https://stopfake.org/en/about-us/, accessed July 9, 2019.
14. "Russia Internet Freedom: Thousands Protest Against Cyber-security Bill," *BBC*, March 10, 2019.
15. Shannon Van Sant, "Russia Criminalizes the Spread of Online News Which 'Disrespects' the Government," NPR, March 18, 2019.
16. Accessnow, #KeepItOn, What is an Internet Shutdown, https://www.accessnow.org/keepiton/, accessed July 12, 2019.
17. *Russia. Internet Freedom 2016: On a War Footing*, Report, AGORA, 2016.
18. GreatFire.org, English Version, https://en.greatfire.org, accessed July 12, 2019.
19. VPNMentor, 5 Best VPNs for Telegram in Russia in 2019 [only those work], https://www.vpnmentor.com/blog/unblock-telegram-russia-with-best-vpns/, for Iran, 5 Best VPNs for Iran, https://www.vpnmentor.com/blog/best-vpns-for-Iran/, for China, 9 Best (Still Working in July 2019) VPNs for China," https://www.vpnmentor.com/blog/5-best-vpns-for-china-verified-list/, accessed July 12, 2019.
20. Lantern, https://getlantern.org/en_US/index.html, accessed July 12, 2019; Deflect, Protecting Online Voices, https://deflect.ca/#our-principles, accessed July 12, 2019.
21. Open Technology Fund, About, https://www.opentech.fund/about, accessed July 11, 2019.
22. Cybersecurity Tech Accord, About: Mission Statement/Values/Signatories, https://cybertechaccord.org/about/, accessed July 11, 2019.

NOTES

23. "Digital Peace in the Age of Cyber Threats," Presentation, Brad Smith, RSA WEB Summit, 2018, Lisbon, Portugal: video 21:30'-21:41', https://www.youtube.com/watch?v=d-k5U2Bd3PQ, accessed July 11, 2019.
24. A US cyber policy that demands the Internet remains open, interoperable, secure, and reliable has been remarkably consistent. See *National Cyber Strategy of the United States of America*, White House, September 2018, 24; Summary, *Department of Defense Cyber Strategy*, DOD, 2018, 1, 7; *Cybersecurity Strategy*, US Department of Homeland Security, May 15, 2018, 4; President Trump, "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," The White House, Office of the Press Secretary, May 11, 2017, Sec. 3 (a); *International Cyberspace Policy Strategy*, Department of State, March 2016, 2; Cyber Strategy, DOD, April 2015, 1; *Strategy for Operating in Cyberspace*, DOD, July 2011, 2; and *International Strategy for Cyberspace*, White House, May 2011, 3, 21.
25. Proclamation, *Paris Call: for Trust and Security in Cyberspace*, November 12, 2018: 1; and see list of signatories.