# Safety & Security

# Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition

Gen. Keith B. Alexander, USA (Ret.), and Jamil N. Jaffer

In late 2015, China announced the creation of its Strategic Support Force (SSF) to unify the People's Liberation Army's (PLA) cyber, space, and electronic warfare capabilities,[1] an effort that parallels the creation of United States Cyber Command (USCYBERCOM) in 2009.[2] Just like the United States, in recent years China has begun to describe cyberspace as a separate domain of warfare and strategic competition.[3] Both China and the United States believe that their respective defense establishments should play a central role in protection of national assets from threats in cyberspace.[4]

According the US Department of Defense, the creation of the SSF likely represents China's "first step in developing a cyber force that creates efficiencies by combining cyber reconnaissance, attack, and defense capabilities into one organization."[5] This likewise parallels the mission of USCYBERCOM—namely, of achieving and maintaining superiority in cyberspace by unifying cyberspace operations, securing data and systems, and providing military options to leadership.[6] Indeed, Chinese military authors cite the development of USCYBERCOM as having successfully combined cyber functions under a single command structure, including the combination of offensive and defense capabilities.[7]

Just as US Secretary of Defense Leon Panetta noted in 2012 that it is the responsibility of the Department of Defense to "defend the nation" in cyberspace,[8] the Chinese view the role of the PLA's SSF as "safeguard[ing] China's interests in new domains such as . . . cyberspace."[9] Furthermore, USCYBERCOM explicitly differentiates its responsibility to "defend the nation" in cyberspace from its offensive capabilities and its support for active military operations.[10] Similarly, Chinese military doctrine writers also differentiate between peacetime defensive operations and wartime military

Gen. Keith B. Alexander, USA (Ret.), is the former director of the National Security Agency and founding commander of the US Cyber Command. General Alexander recently served as a member of the President's Task Force on Enhancing National Cybersecurity and currently serves as president and CEO of IronNet Cybersecurity, a startup cybersecurity firm, as well as in a number of other public and private roles.

Jamil N. Jaffer is the former chief counsel and senior advisor to the Senate Foreign Relations Committee and senior counsel to the House Intelligence Committee as well as an associate counsel to President George W. Bush. Mr. Jaffer currently serves as founder of the National Security Institute at the Scalia Law School at George Mason University and as a visiting fellow at the Hoover Institution as well as a vice president at IronNet Cybersecurity. Certain portions of this paper—in particular the section on creating a more defensible national cyber ecosystem—are drawn directly or principally from testimony presented by General Alexander on April 11, 2018, before the House Armed Services Committee.

support and offensive operations.[11] At the same time, newer, evolving doctrine in both nations also recognizes that in the cyber domain—as well as in others—the current status quo represents more of a state of "continuous competition" rather than the traditional war-versus-peace paradigm[12] and also understands the cyber battlespace as one where the lines between defense and offense are increasingly fluid.[13]

Given that one primary goal of the SSF is to accelerate the development of Chinese offensive and defensive cyber capabilities,[14] and given the rise of a number of other peer and near-peer competitors in cyberspace,[15] as well as the inherently asymmetric nature of cyber capabilities, a key question for the United States is how it can maintain the relative dominance it has enjoyed in this new domain of warfare going forward.[16] The reality today is that America's relative hegemony in cyberspace as a domain of warfare is being (and will continue to be) contested in cyberspace. Today, the United States faces strategic threats in cyberspace from China as well as from Russia, two longtime key adversaries in this domain.[17] The United States and its allies also face tactical threats from a range of actors including increasingly active nation-states like North Korea and Iran as well as a wide array of non-state actors, from criminal gangs to terrorist groups.[18] And some of these latter actors are working on behalf of, or alongside, the nation-states that are also operating against the United States in the cyber domain.[19]

**Newer, evolving doctrine in both nations also recognizes that in the cyber domain—as well as in others—the current status quo represents more of a state of "continuous competition" rather than the traditional war-versus-peace paradigm and also understands the cyber battlespace as one where the lines between defense and offense are increasingly fluid.**

**A key question for the United States is how it can maintain the relative dominance it has enjoyed in this new domain of warfare going forward.**

This paper argues that the best route to continued success for the United States in the cyber domain is to (1) create a more defensible national ecosystem at home and in partnership with key allies; (2) continue to invest significant resources in cyber intelligence collection, offensive and defensive cyber capability development, and game-changing capabilities, including cognitive computing and quantum systems; and (3) create a sustainable deterrence capability in the cyber realm.

## Creating a More Defensible National Cyber Ecosystem

In the modern era, it is critically important that governments fundamentally rethink their architectures for cyber defense. The reality is not only that nation-states like the United States and China view cyberspace doctrinally as a domain for warfare but also that globally cyberspace has become an actual domain of conflict. Indeed, the United States and its allies are very much in the throes today of a series of ongoing—albeit low-level—conflicts in cyberspace.[20] Moreover, these cyber conflicts not only have a classic political component to them but, in many instances, they also have a significant economic component. For example, in the case of China, the United States has long known that its economic security is being directly challenged through the use of

Chinese government cyber capabilities to siphon off massive amounts of economic wealth through the theft and coerced transfer of intellectual property that is at the heart of the modern American economy.[21] In recognition of the critically important role that economic capabilities play, the recently released National Security Strategy makes clear that the United States views economic security as part and parcel of its national security interests.[22] Moreover, the United States is hardly alone among its allies in facing down such threats. Japan and South Korea, for example, have both recently suffered significant economic theft in the form of cryptocurrency hacking allegedly undertaken by North Korea.[23]

At the same time, economic threats are not the only challenges facing the United States and its allies in cyberspace. The national security of America and its allies is also directly threatened by nations like Russia, which have engaged in obvious efforts to undermine confidence in the American political system.[24] Russia has sought to embed long-term penetrations in critical infrastructure sectors in order to conduct espionage and prepare the battlespace for potential future conflict scenarios,[25] and has conducted what our government recently referred to as the most "destructive and costly cyber-attack in history."[26] Concerns raised by these classic economic and political threats are further enhanced by the fact that nation-states like Iran[27] and North Korea,[28] which typically would not be viewed as near-peer competitors to the United States and its allies in the cyber domain, are nonetheless conducting significant cyber-attacks on United States soil and against American allies.[29]

Given this range of threats and the fact that the United States and other nations find themselves currently in the middle of a very real series of (albeit minor) military skirmishes in cyberspace, it may be surprising that the United States still finds itself challenged in providing "for the common defense" of the nation in the cyber domain.[30] The challenges in the United States do not primarily relate to a lack of forces or capabilities.[31] To the contrary, the creation of US Cyber Command in 2009 provides the United States with very real and robust capabilities in both the offensive and defensive areas, capabilities that have the ability to both protect the United States writ large and to make cyber deterrence a reality in the global arena.[32]

**The national security of America and its allies is also directly threatened by nations like Russia, which have engaged in obvious efforts to undermine confidence in the American political system.**

At least in the United States, the challenges to creating a more defensible national cybersecurity ecosystem relate principally to how core roles, responsibilities, and authorities are allocated. In particular, the United States faces two core challenges when it comes to cyberspace: how to organize as a government to defend and fight in this domain, and how to build jointness against

**The challenges in the United States do not primarily relate to a lack of forces or capabilities. To the contrary, the creation of US Cyber Command in 2009 provides the United States with very real and robust capabilities in both the offensive and defensive areas, capabilities that have the ability to both protect the United States writ large and to make cyber deterrence a reality in the global arena.**

cyber-attacks between the public and private sectors during conflicts that require acting with both speed and vigor to defend the nation.[33]

One principal challenge facing the United States is that USCYBERCOM—ostensibly charged since 2012 with the mission of defending the nation against cyber-attacks—lacks clear authority and rules of engagement (ROE).[34] The goal should not be to respond to an attack but rather to protect against an attack before damage to infrastructure occurs. Given the speed at which cyber conflicts take place, governments need to ensure that warfighters can act with speed and agility to stop an attack before an enemy strikes, as well as respond effectively to an attack in progress. This requires advance authority for USCYBERCOM to take action and clear ROE that provide a broad range of options to use in appropriate circumstances while also limiting action to appropriate bounds outside the United States. Although the idea of providing advance authority to take action that admittedly might spark a larger conflict is almost certainly controversial, if structured properly with appropriate limitations, effective civilian oversight, and significant, timely reporting to the legislative branch, many of the key concerns can be effectively mitigated.[35] Similarly, within the United States, agencies like the Federal Bureau of Investigation will need advance authority to take action domestically against potential cyber actors who are utilizing co-opted infrastructure located at home.

At the same time, simply providing USCYBERCOM and other agencies with robust authorities and solid ROEs is not enough.[36] Because the vast majority of American cyber infrastructure is owned and operated by the private sector, in order to defend the nation, the government must work closely with the private sector by setting the conditions for a truly defensible cyber infrastructure. This would include empowering private sector defensive capabilities and providing for interoperable capabilities that can be used if a national crisis requires direct government assistance to industry, as well as joint exercises to test out such operations.[37]

The fact is that no single entity—whether a private sector company or a government agency—can stand alone against the most capable threat actors.[38] Indeed, in no other area do we expect individual private companies to defend themselves against nation-states.[39] For example, while we reasonably expect private corporations to have high fences and armed guards around their warehouses to protect against thieves, we don't expect those same companies to have surface-to-air missiles on their warehouses to defend against foreign bombers dropping ordnance.[40] When it comes to cyberspace, however, we expect exactly that: individual companies, standing alone, are expected to defend themselves against all comers, from script kiddies to nation-states.[41] This is a policy destined to fail under its own weight.[42]

Rather than rely on private companies to defend themselves alone against such serious actors, governments should move to a collective defense architecture both within the private sector as well as between the public and private sectors.[43] The first step would be industries sharing information on cyber threats at scale and speed within and across critical sectors and then, over time, between governments and the private sector more generally.[44] Indeed, in order to stop an attack before it happens, governments need to be able to assess their enemy's plans, intentions, and capabilities and must be able to identify the attacks as they are progressing but before they actually have an impact. In many ways, the visibility needed to stop an attack before it has an impact can be analogized to the national air traffic control system.[45] Successful, robust sharing of cyber-threat

data between the government and industry can help empower the development of such a cyber common operational picture.[46] Just as the air traffic control picture ensures aviation safety and helps synchronize government and civil flights, a cyber common operational picture can help synchronize our national common cyber defense and enable rapid response in a time of crisis.[47] In the United States, the energy and financial sectors, working collaboratively with government-funded institutions[48] and outside providers,[49] are beginning to lead in this space by creating robust information sharing collaborations both internally to these sectors, as well as with the government.[50]

Beyond creating a common operational picture, governments can also assist industry more directly.[51] They can do so by sharing cyber-threat information with the private sector in real time and at machine speed.[52] In addition, governments could use their overseas intelligence-collection architectures to collect on threats to their private sector and pass on this information—even in its highly classified form—to home industry so that it may be used to defend the nation's economic base.[53]

Finally, governments and private industry ought to work together to develop interoperable capabilities that can be utilized in a crisis.[54] Such interoperable capabilities would allow governments to directly provide assistance to the private sector and utilize appropriate governmental authorities to respond to attacks in progress.[55] Moreover, exercising these capabilities in advance of an actual threat would allow both governments and private industry to be prepared in actual cyber conflict scenario.[56]

**Governments and private industry ought to work together to develop interoperable capabilities that can be utilized in a crisis.**

## Investing Resources in Key Cyber Capabilities

Both the United States and China have made clear that they expect to invest significant resources in building cyber capabilities in the near term.[57] The same is true for many actors around the world, including edge competitors like Iran and North Korea. As a result, significant investment in key areas will be required for the United States and its allies to continue to maintain their collective lead in cyberspace and to ensure more comprehensive national defense across the board. Some of the key areas for such investment ought to include improving cyber intelligence collection, achieving better attribution capabilities, creating advanced offensive and defensive cyber capabilities, and expanding on game-changing capabilities, including artificial intelligence and cognitive computing.

Improved intelligence collection overseas is a minimum first step for all nations seeking to address significant threats facing them in cyberspace. If a nation is able to understand the potential threats facing both its government as well as its private industry, it will be better placed to defend against such threats in the first instance and to take action to respond as needed. Such intelligence collection can also provide advance warning of a potential threat or may provide attribution of an attack in progress or when completed.

While many of the nation-states operating against the United States and its allies in cyberspace have long sought to escape detection by concealing their activities through the use of non-attributable organizations and infrastructure, as well as the use

of co-opted systems,[58] the United States and other nations have committed significant resources to addressing the attribution problem and have increased their ability to more reliably attribute attacks.[59] Indeed, recent authoritative attributions by the US government of certain major attacks to nation-state actors, from WannaCry to North Korea to NotPetya to Russia, as well as a number of others, highlight this newer trend.[60] At the same time, the reality for the United States and allied governments is that key actors, including Russia and China, are aggressively targeting non-governmental entities, particularly critical infrastructure providers, for which the government has limited access to data. Similarly, many of the hop points (computers used by attackers to obscure where the attacks originate) that are being used by attackers—whether nation-states or otherwise—reside on private sector networks. Governments like the United States often cannot directly access such hop points, whether for legal or operational reasons. As such, in order to truly extend its attribution capabilities, the US government and others must work closely with private industry in order to truly understand the nature and scope of attacks. Such collaboration will allow both industry and government to benefit from combining information about what is taking place inside the United States or other allied nations with the information collected overseas by their intelligence agencies to better attribute attacks and to prevent further incidents.

**As such, in order to truly extend its attribution capabilities, the US government and others must work closely with private industry in order to truly understand the nature and scope of attacks. Such collaboration will allow both industry and government to benefit from combining information about what is taking place inside the United States or other allied nations with the information collected overseas by their intelligence agencies to better attribute attacks and to prevent further incidents.**

Developing advanced offensive and defensive capabilities is likewise critical for further investment by the United States and its allies. Recent attacks have demonstrated that nation-states and non-nation-states alike have developed the ability to repurpose leaked foreign nation-state capabilities to their own ends as well as to develop significant new intelligence tools domestically. Being able to effectively defend against such nation-state-level capabilities is likely to be an important tool for cyber defenders going forward. At the same time, having the demonstrated capacity to use offensive cyber tools will likely be necessary to deter other states, including states that can't be deterred by other means like diplomatic pressure or sanctions.

Finally, continuing to invest in and leverage game-changing capabilities, including cognitive computing and quantum systems, will be critical to maintaining the US and allied edge in cyberspace. The reality is that application of these capabilities has the ability to fundamentally and rapidly change the cyber battlespace. In particular, effective application of cognitive computing—which seeks to model human thought processes using computers—to large amounts of cyber-threat data can provide the ability to evaluate next steps that might be taken to defend against an evolving threat. Specifically, in a scenario in which a nation-state is able to attribute a particular pattern of behavior around a set of attacks, the application of cognitive computing may permit the defender to get ahead of future attacks

or to identify them earlier in the kill chain. Similarly, the potential use of such capabilities to calculate a series of possible outcomes in a given threat scenario, such as the probability of adversary success, could also provide cyber defenders with hugely valuable information. In addition, the potential use of quantum capabilities—which apply certain aspects of quantum physics to allow computers to accomplish calculations much faster than is currently possible—to defeat encrypted malware could also provide cyber defenders with valuable information. This is so because aspects of today's most common encryption methodologies are based on the inability of current systems to rapidly conduct calculations against certain very large numbers (e.g., finding the prime factors of a very large number). Thus, if quantum computing allows much more rapid calculations against such numbers, key aspects of modern encryption—including that used to encrypt malware—may become significantly more vulnerable.[61]

## Creating a Sustainable Cyber Deterrence Capability

Deterrence in cyberspace also represents a key strategic area of focus for Chinese military scholars and war planners,[62] as it does in the United States.[63] The actual consequences of the application of traditional deterrence theory in cyberspace today remain somewhat opaque. While it is clear that nation-states with leading cyber capabilities like the United States, China, and Russia are not currently prepared to utilize their most robust capabilities against what they perceive as peer competitors because they do fear a potential response, it is also clear that other nations are willing to take specific limited actions that, in other contexts, might be seen as crossing the line against such major players. For example, the destructive nature of attacks undertaken in the continental United States against certain American private sector companies by Iran and North Korea[64] represents a calculation (apparently correct—at least to date) by those nations that such action would not provoke a major response. Likewise, major nations appear to have taken the view that significant cyber activities against non-peer competitors, like Russia's attacks against Estonia and Ukraine,[65] would likewise not provoke an effective response, whether by those nations or other nations with the ability to respond. At least in the latter scenario, the calculation that peer competitors would not risk a major confrontation over edge states or that such peer competitors remain concerned with their own cyber exposure to respond in that domain, appears also to have been correct. Lastly, at least in one instance, major nation-states *have* faced off in cyberspace, with Russia assessing that its manipulation of American public opinion through social media during the 2016 elections would not provoke a significant American response.[66] In that case, we have seen a significant response in the form of public criticism, sanctions, expulsions of intelligence officers, and closure of diplomatic facilities, but we have yet to see the type of response that is likely to effectively limit such efforts in the future.

In order to effectively deter attacks in cyberspace, the United States and its allies must be willing to increasingly describe some measure of the nature and scope of their capabilities in the cyber domain and to set out specific criteria under which cyber-attacks may be responded to and the potential nature of such responses.[67] Moreover, the government must be prepared to actually respond when such attacks take place. Today, little if any information is intentionally made public about the nature of the US's strategic and tactical capabilities in cyberspace. Indeed, what little is known

largely comes from leaks related to alleged cyber operations. The same is largely true of American allies. And while it is without question that the United States and its allies reserve the right to respond to cyber operations conducted against them, refusing to provide insight into some of the nation's capabilities in this arena makes it nearly impossible to credibly leverage deterrence based on a potential cyber-based response.

Similarly, without an understanding or a declared policy of certain redlines with respect to cyber operations, potential threat actors are left to guess about what actions might trigger a response and what the nature of that response might be. While strategic ambiguity has its place in international relations, it is most effective when such ambiguity is on the edges of a fairly clear policy. At the present time, in the cyber domain, given that little is understood about when and how nations may respond, it is unsurprising that we see various nations testing the boundaries and engaging in operations that may otherwise be deterred if it were understood that a clear response would be forthcoming. If the United States and its allies are able to agree to a basic set of rules of the road, this framework could create the basis for a sustainable deterrence architecture. The basic elements of such a set of rules can be based on analogies to traditional military or intelligence activities—cyber-attacks causing significant loss of life, physical damage to infrastructure, or significant financial harm or loss would be actionable, whereas traditional forms of espionage, such as a theft of government defense or foreign policy information, would not be. The obvious challenge to such an effort would be the more equivocal cases, such as attempts to influence public opinion, theft of significant amounts of intellectual property, attacks that cause limited physical damage, or efforts to penetrate infrastructure for long-term access versus immediate action, all of which may reasonably be analogized to traditional actions that may or may not provoke a response. The fact that these cases create a significant challenge, however, is not a reason to avoid making tough choices about how the United States and its allies ought to react to malicious cyber activities. To the contrary, the fact that there remains ambiguity in this area and that US and allied responses have been limited (at least in the public space) to date means that other nations are more likely to continue to probe our boundaries.

**Similarly, without an understanding or a declared policy of certain redlines with respect to cyber operations, potential threat actors are left to guess about what actions might trigger a response and what the nature of that response might be. While strategic ambiguity has its place in international relations, it is most effective when such ambiguity is on the edges of a fairly clear policy.**

Finally, as with all forms of deterrence, cyber deterrence will be effective only to the extent that nation-states are willing to stand by the redlines they set and actually enforce them. At the same time, long-term deterrence can be dramatically undermined where nation-states set unwise redlines or create redlines that they are not actually willing to enforce, as in the case of Syria's use of chemical weapons in 2012–13. As such, in cyberspace, significant attention must be given to establishing clear boundaries and setting out clear consequences only where governments are actually prepared and willing to take action.

## Conclusion

The establishment of the SSF by China, which was informed by the creation of USCYBERCOM in the United States, highlights the importance of the United States and its allies undertaking a concerted effort to maintain their collective edge in the cyber domain. This will require a significant rethinking of the roles and responsibilities of the government and the private sector when it comes to cyber defense. It will demand significant investment in new, advanced capabilities and a new approach to deterrence in the cyber arena. All of these changes are within the realm of the possible, but significant barriers to success remain, including fundamental disconnects within the American political system and between the defense, intelligence, and homeland security communities in the government. Thus, if the United States is to maintain its relative dominance in cyberspace over the long term, it is likely to require a sustained commitment from the leadership of the executive branch and the commitment of a significant amount of political and financial resources in the near term.

## Notes

1. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017* (Department of Defense, 2017), 34, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF; Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the Strategic Support Force (SSF) and Its Implications for Chinese Military Space Operations* (RAND Project Air Force, 2017), iii, https://www.rand.org/pubs/research_reports/RR2058.html. (noting that the SSF was "announced on December 31, 2015" and is "charged with overseeing Chinese military space, cyber, and electronic warfare capabilities.")
2. Secretary of Defense, *Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations* (Department of Defense, 2009), http://online.wsj.com/public/resources/documents/OSD05914.pdf. ("Our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.")
3. Department of Defense, *Military and Security Developments*, 35 ("The PLA in recent years has emphasized the importance of cyberspace as a new domain of national security and arena for strategic competition. China's 2015 defense white paper identified cyberspace as one of four 'critical security domains' alongside the far seas, space, and nuclear domains."); The White House, *National Security Strategy of the United States of America* (The White House, 2017), 8, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. ("State and non-state actors place the safety of the American people and the Nation's economic vitality at risk by exploiting vulnerabilities across the land, air, maritime, space, and cyberspace domains. Adversaries constantly evolve their methods to threaten the United States and our citizens. We must be agile and adaptable.")
4. Pollpeter, Chase, and Heginbotham, *Creation of the Strategic Support Force*, 23. (quoting an article from the *Liberation Army Daily* as saying "In order to meet the requirements of building a strong space power and a strong cyber power, the Strategic Support Force was established to create a new type of operational force that can protect the country's security."); Department of Defense, *The Department of Defense Cyber*

*Strategy* (Department of Defense, 2015), 2, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. ("In concert with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. . . . To this end the Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.")

5. Department of Defense, *Military and Security Developments*, 35.
6. US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (US Cyber Command, 2018), 1, https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf. (describing the basic mission of USCYBERCOM: "to achieve and maintain superiority in cyberspace . . . [to] synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners . . . [to] demonstrate our resolve against cyberspace threats . . . [to] unify cyberspace operations . . . [to] secure networks, platforms, and data . . . [and to] expand the military options available to national leaders and operational commanders.")
7. Department of Defense, *Military and Security Developments*, 35. ("PLA writings reference U.S. Cyber Command as effectively consolidating cyber functions under a single entity and streamlining leadership. They acknowledge the benefits of unifying leadership, centralizing the management of cyber resources, and combining its offensive and defensive cyber capabilities under one military organization.")
8. Department of Defense, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," last modified October 11, 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
9. Department of Defense, *Military and Security Developments*, 39.
10. Department of Defense, "Fact Sheet: The Department of Defense (DoD) Cyber Strategy," last modified April, 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf. (describing "DoD's three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans").
11. Department of Defense, *Military and Security Developments*, 35. ("PLA writings distinguish between peacetime and wartime cyber operations. In peacetime, PLA cyber missions include 'defending electromagnetic space and cyberspace' because of China's increasing reliance on the information economy. During wartime, cyber capabilities can 'help the PLA understand the enemy's trend, help the troops plan the combat operations, and ensure victory on the battlefield,' according to one PLA scholar.")
12. See, e.g., The White House, *National Security Strategy*, 28. ("China, Russia, and other state and nonstate actors recognize that the United States often views the world in binary terms, with states being either 'at peace' or 'at war,' when it is actually an arena of continuous competition."); Pollpeter, Chase, and Heginbotham, *Creation of the Strategic Support Force*, 23. (noting the "designation of outer space and cyberspace by [a Chinese] 2015 defense white paper as domains that 'have become new commanding heights in strategic competition.'")
13. US Cyber Command, *Command Vision,* 6. ("Superiority through persistence . . . describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace."); Annie Kowalewski, "China's Evolving Cybersecurity Strategy," *Georgetown Security Studies Review*, last modified October 27, 2017, http://georgetownsecuritystudiesreview.org/2017/10/27/chinas

-evolving-cybersecurity-strategy/. ("China sees an opportunity to gain an advantage against other large powers in, and beyond, the cyber domain. This asymmetric capability can be used for deterrence purposes, gaining an economic advantage, or even 'winning wars' without actually fighting. That is, an overwhelming defensive and offensive Chinese cyber capability can stop the threat of foreign influence and intervention via the threat of use, such as attacks on critical infrastructure, or by undermining an opponent's ability to organize by striking before an opponent can attack. China thus views cyber as both a necessary defensive capability and as a weapon that can be utilized during both peacetime and war.")

14. Department of Defense, *Military and Security Developments*, 34. (noting that "[d]uring the SSF's establishment ceremony, President Xi described it as a 'new-type combat force to maintain national security and an important growth point for the PLA's combat capabilities'" and arguing that China's establishment of the SSF demonstrates "its commitment to 'expedite the development of a cyber force'")
15. US Cyber Command, *Command Vision,* 2. ("As the nation's cyber warriors, USCYBERCOM operates daily in cyberspace against capable adversaries, some of whom are now near-peer competitors in this domain.")
16. See, e.g., The White House, *National Security Strategy,* 27. ("The spread of accurate and inexpensive weapons and the use of cyber tools have allowed state and non-state competitors to harm the United States across various domains. Such capabilities contest what was until recently U.S. dominance across the land, air, maritime, space, and cyberspace domains.")
17. Keith B. Alexander, "Written Testimony on Cyber Warfare Today: Preparing for 21st Century Challenges in an Information-Enabled Society" US House Armed Services Committee, last modified April 11, 2018, https://docs.house.gov/meetings/AS/AS00/20180411/108077/HHRG-115-AS00-Wstate-AlexanderK-20180411.pdf.
18. Ibid.
19. Ibid.
20. Ibid.; Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, March, 2018), 5–6, https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA—-Unclassified—SASC.pdf. ("The risk is growing that some adversaries will conduct cyber-attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war. . . . Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations . . . . The use of cyber-attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber-attacks that pose growing threats to the United States and US partners.")
21. Dennis C. Blair and Keith Alexander, "China's Intellectual Property Theft Must Stop," *New York Times,* August 15, 2017, https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html. ("Chinese companies, with the encouragement of official Chinese policy and often the active participation of government personnel, have been pillaging the intellectual property of American companies. Altogether, intellectual-property theft costs America up to $600 billion a year, the greatest transfer of wealth in history. China accounts for most of that loss."); Alexander, "Cyber Warfare Today"; The White House, "Remarks by President Trump at Signing of a Presidential Memorandum Targeting China's Economic Aggression," last modified March 22, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-presidential-memorandum-targeting-chinas-economic-aggression/. (statement of US Trade Representative Robert Lighthizer: "Lighthizer: . . . Technology is probably the most important part of our economy. There's 44 million people who work

in high-tech knowledge areas. No country has as much technology-intensive industry as the United States. And technology is really the backbone of the future of the American economy. . . . And we concluded that, in fact, China does have a policy of forced technology transfer; of requiring licensing at less than economic value; of state capitalism, wherein they go in and buy technology in the United States in non-economic ways; and then, finally, of cyber theft.")

22. The White House, *National Security Strategy,* 17. (quoting President Trump as saying in November 2017, "Economic security is national security" and noting that "a strong economy protects the American people, supports our way of life, and sustains American power . . . [and a] growing and innovative economy allows the United States to maintain the world's most powerful military and protect our homeland.")
23. "South Korean Intelligence Says N. Korean Hackers Possibly behind Coincheck Heist—Sources," Reuters, February 5, 2018. ("South Korea's intelligence agency told lawmakers North Korean hackers could have been behind the $530 million theft of virtual coins from a Japanese cryptocurrency exchange last month, people familiar with the matter told Reuters on Tuesday . . . A South Korean lawmaker on Monday said North Koreans were responsible for billions lost in theft from local cryptocurrency exchanges in 2017."). See also Luke McNamara, "Why Is North Korea So Interested in Bitcoin?," *FireEye Blog*, September 11, 2017, https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html. ("We may be witnessing a second wave of this campaign: [North Korean] state-sponsored actors seeking to steal bitcoin and other virtual currencies as a means of evading sanctions and obtaining hard currencies to fund the regime. Since May 2017, we have observed North Korean actors target at least three South Korean cryptocurrency exchanges with the suspected intent of stealing funds. . . . [I]t should be no surprise that cryptocurrencies, as an emerging asset class, are becoming a target of interest by a regime that operates in many ways like a criminal enterprise.")
24. Alexander, "Cyber Warfare Today," 2; US Department of Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," press release, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312. ("Today's action counters Russia's continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018, in statements released by the White House and the British Government.")
25. Ibid.; Department of Homeland Security, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," alert no. TA18-074A, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A. ("This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. . . . DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).". See also Coats, *Worldwide Threat Assessment* (2018). ("In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.")
26. Ibid.; The White House, "Statement from the Press Secretary," last modified February 15, 2018), https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/. ("In June 2017, the Russian military launched the most destructive and costly cyber-attack

in history. . . . The attack, dubbed 'NotPetya,' quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas.")

27. See, e.g., Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, May, 2017), 1–2, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf. ("For example, in 2013, an Iranian hacker conducted an intrusion into the industrial control system of a US dam, and in 2014, Iranian actors conducted a data deletion attack against the network of a US-based casino."); Coats, *Worldwide Threat Assessment* (2018), 6. ("Iran's cyber-attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector."); Alexander, "Cyber Warfare Today," 3; Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," press release no. 18-350, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary. (describing Iranian hackers that "conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund.")
28. Alexander, "Cyber Warfare Today," 3; The White House, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," last modified December 17, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/. ("In May of this year, a dangerous cyberattack known as WannaCry spread rapidly and indiscriminately across the world. The malware encrypted and rendered useless hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries. . . . This was a careless and reckless attack. It affected individuals, industry, governments. And the consequences were beyond economic. The computers affected badly in the UK and their healthcare system put lives at risk, not just money. After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea."). See also Coats, *Worldwide Threat Assessment* (2017), 2. ("Pyongyang has previously conducted cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyber-attacks to support its political objectives.")
29. Ibid.
30. US Constitution preamble.
31. Alexander, "Cyber Warfare Today," 3.
32. Ibid.
33. Ibid., 3–4.
34. Ibid., 4.
35. Ibid.
36. Ibid.
37. Ibid.
38. Ibid.
39. Ibid., 5.
40. Ibid.; Keith B. Alexander, Jamil N. Jaffer, and Jennifer S. Brunet, "Clear Thinking about Protecting the Nation in the Cyber Domain," *Cyber Defense Review* 2, no. 1 (2017): 29, 33. ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks. For example, we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD. Today, however, in cyberspace, that expectation is flipped on its head.")

41. Ibid.
42. Ibid.
43. Ibid.
44. Ibid.
45. Ibid., 6.
46. Ibid.
47. Ibid.
48. See "Energy Sector Cybersecurity Preparedness," Department of Energy, https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0. ("The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE and industry and managed by the Electricity Information Sharing and Analysis Center (E-ISAC). The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the nation's Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental U.S. electricity subsector customers.")
49. See, e.g., "IronNet Cybersecurity Announces Significant Product Advancements Enhancing the Protection of National Critical Infrastructure and $78 Million Series B Funding to Accelerate Advancement and Adoption," IronNet Cybersecurity, last modified May 2, 2018, https://ironnetcyber.com/press-release/2018-05-02-IronNet-Cybersecurity-Raises-Series-B. ("IronNet announced for the first time publicly the standup, effective late last year, of its proprietary IronDome collective defense system by nearly a half-dozen multi-state energy sector providers covering well over a dozen operating subsidiaries across more than two dozen states. IronDome is providing this key sector of national critical infrastructure with automated, real-time sharing of cyber event data and analysis between all of its participating energy company partners, which together provide energy service to half of the country.")
50. Ibid., 5.
51. See Alexander, "Cyber Warfare Today," 6.
52. Ibid.
53. Ibid.
54. Ibid.
55. Ibid.
56. Ibid.
57. See The White House, *National Security Strategy,* 30. ("The Department of Defense must develop new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains, including against those operating below the level of conventional military conflict.")
58. See, e.g., John A. Serabian Jr., "Statement for the Record on Cyber Threats and the US Economy," Joint Economic Committee on Cyber Threats and the US Economy, last modified February 23, 2000, https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html. ("Technology permits an attacker to conceal points of origin by hopping through several intermediate way stations in cyber space—including international cyber space—making identification of an attacker a daunting challenge. An attacker can spoof or conceal the origin of the individual hops and erase cyber footprints from victim computers. . . . Thus, unlike the threats of the cold war, cyber threats can come from almost anywhere. They can originate from any location, affect systems anywhere in the world, disguise origins and travel routes, and do it all instantaneously. CIA focuses on threats overseas, but it is often difficult until very late in a given scenario to know whether an attack ultimately originated overseas or if an overseas computer is merely an intermediate step.")
59. See, e.g., The White House, *National Security Strategy,* 32. ("We will invest in capabilities to support and improve our ability to attribute cyberattacks, to allow for rapid response.")
60. See, e.g., The White House, "WannaCry Malware Attack"; The White House, "Statement from the Press Secretary."
61. It is worth noting, in this context, that many

have also argued that the development of quantum computing can make certain aspects of encryption even stronger (e.g., through the use of quantum key distribution, which could permit the secure distribution of symmetric encryption keys), so the net effects on encryption of the potential development of widely available quantum computing remains unclear at best. See, e.g., "What Is Quantum Key Distribution?," Cloud Security Alliance, last modified 2016, https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/CSA_What%20is%20Quantum%20Key%20Distribution_QSS.pdf.

62. See Pollpeter, Chase, and Heginbotham, *Creation of the Strategic Support Force*, 32. ("Because PLA strategists view space and cyber warfare as important components of strategic deterrence alongside nuclear and conventional forces, the SSF would also appear to be poised to play an important role in China's further development of its strategic deterrence posture and in the conduct of deterrence operations."); Department of Defense, *Military and Security Developments*, 35. ("PLA scholars continue to explore new concepts in cyberspace, such as deterrence in cyberspace."); The White House, *National Security Strategy,* 27 ("Deterrence today is significantly more complex to achieve than during the Cold War. Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses. The spread of accurate and inexpensive weapons and the use of cyber tools have allowed state and non-state competitors to harm the United States across various domains. Such capabilities contest what was until recently U.S. dominance across the land, air, maritime, space, and cyberspace domains. They also enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces. Deterrence must be extended across all of these domains and must address all possible strategic attacks.")
63. Department of Defense, "Cyber Strategy," 1. ("This strategy describes the Department of Defense contributions to a broader national set of capabilities to deter adversaries from conducting cyberattacks. The Department of Defense assumes that the deterrence of cyberattacks on U.S. interests will be achieved through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. DoD has a number of specific roles to play in this equation; this strategy describes how DoD will fulfill its deterrence responsibilities effectively.")
64. See, e.g., Coats, *Worldwide Threat Assessment* (2017), 1–2. ("In 2014, Iranian actors conducted a data deletion attack against the network of a US-based casino. . . . Pyongyang has previously conducted cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyber-attacks to support its political objectives.")
65. Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," NBC News, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111. ("In the past decade the Russian government has mounted more than a dozen significant cyber-attacks against foreign countries . . . to project Russian power. Starting in 2007, the Russians attacked former Soviet satellites like Estonia, Georgia, and Ukraine, and then branched out to Western nations like the U.S. and Germany. . . . Russia has shut down whole segments of cyber space to punish or threaten countries.")
66. *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections* (Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf. ("We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election . . . Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential

election, including targets associated with both major US political parties."); *Report on Russian Active Measures* (House Permanent Select Committee on Intelligence, 2018), viii, https://docs.house.gov/meetings/IG/IG00/20180322/108023/HRPT-115-1.pdf. ("In 2015, Russia began engaging in a covert influence campaign aimed at the U.S. presidential election. The Russian government, at the direction of President Vladimir Putin, sought to sow discord in American society and undermine our faith in the democratic process . . . While the 2016 U.S. presidential election helped focus American attention on Russian cyber and information operations, the Russian government has conducted active measure campaigns in Europe for years.")

67. For an initial attempt at getting the Department of Defense to set out such a policy, see National Defense Authorization Act for FY 2018, P.L. 115-91, Sect. 1644 (December 12, 2017) (requiring the conduct of a cyber posture review that includes "a declaratory policy relating to the responses of the United States to cyber-attacks of significant consequence. . . . [g]uidance for the development of a cyber deterrence strategy (which may include activities, capability efforts, and operations other than cyber activities, cyber capability efforts, and cyber operations)").