NATIONAL CYBER DEFENSE CENTER

A Key Next Step toward a Whole-of-Nation Approach to Cybersecurity

National Security Perspective

James N. Miller | Robert J. Butler

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

NATIONAL CYBER DEFENSE CENTER

A Key Next Step toward a Whole-of-Nation Approach to Cybersecurity

James N. Miller

Robert J. Butler

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective contains the best opinion of the author(s) at time of issue. It does not necessarily represent the opinion of JHU/APL sponsors.

The views expressed are solely those of the authors and not of any US governmental agencies or departments.

NSAD-R-21-003

Contents

Figures

Tables

Summary

A National Cyber Defense Center (NCDC) would plan and coordinate US government cyber defense operations below the threshold of armed conflict while also conducting contingency planning, and if necessary coordinating national cyber defense operations in the event of armed conflict. The center would plan and coordinate across four key lines of operation, which are essential both below the level of armed conflict and in crisis or war: cyber deterrence, active cyber defense, offensive cyber operations in support of defense, and cyber incident management. To be most effective, the NCDC should be placed in the Office of the National Cyber Director (ONCD), which was established by Congress in late 2020 as a new element of the Executive Office of the President.

Serious and Growing Cyber Threats to US National Security

Both state and nonstate adversaries are conducting sustained cyber-enabled campaigns that aim to advance those adversaries' interests and undermine the interests of the United States. The fabric of American society and the US political system are under attack in cyberspace, as Russia and other countries are conducting cyber-enabled disinformation attacks to sow domestic discord and undermine democracy in the United States. China's cyber-enabled theft of US intellectual property has been estimated to cost the United States 1–2 percent of its gross domestic product annually. The US government and private sector are also vulnerable to disruptive and destructive cyber attacks, as exemplified by Iran's distributed denial-of-service (DDoS) attacks on Wall Street from 2012 to 2013 and North Korea's 2014 cyber attack on Sony Entertainment and its WannaCry ransomware attacks of 2017. Cyber crime costs US firms hundreds of billions of dollars per year; cyber ransomware attacks threaten business operations, and those targeting the health care industry have disrupted hospitals and put patients at risk. The failure to stem cyber intrusions, as exemplified by Russia's massive SolarWinds hack discovered in late 2020 and the hack of Microsoft Exchange discovered in early 2021 (and attributed by many to China), poses incalculable risks to American security.

In addition to the day-to-day challenges from malicious cyber activity below the threshold of armed conflict, US adversaries, particularly China and Russia, have extensively infiltrated US critical infrastructure with implanted cyber capabilities. In the event of a severe crisis or conflict, China and Russia could use cyber weapons to hobble the US military, cripple the US economy, and conduct all-out cyber-enabled disinformation and deception efforts to attempt to sow discord among the American people. If the United States does not posture itself better to be able to prevent and rapidly remediate such cyber attacks, some of which would likely be conducted from infrastructure within the United States, US deterrence of coercion or armed aggression against US allies and partners will be undermined.

Evolving US Cyber Defense Strategy

Over the past three decades, the US government's approach to cybersecurity has evolved significantly. Initially focused at the advent of the information age in the late 1980s on reducing the vulnerabilities of telecommunications and information technology directly supporting national security systems, US strategy broadened in the late 1990s to attempt to reduce the vulnerabilities of the increasingly extensive

networks relied on by both the US government and privately owned US critical infrastructure. As serious cyber attacks below the level of armed conflict mounted in the early 2000s, it became clear that critical infrastructure vulnerabilities were likely to remain for many years. Thus, while continued passive cyber defense efforts (e.g., firewalls, antivirus software, training of personnel to reduce the incidence of "phishing" attacks) were necessary, it was increasingly evident that they were not sufficient.

By 2017, it was clear to many observers, including those in Congress, that a new approach to cyber defense was needed. Over the past several years, the Department of Defense (DoD), led by US Cyber Command and the National Security Agency, has pursued a "Defend Forward" strategy that aims to thwart cyber intrusions and cyber-enabled disinformation attacks by uncovering adversary cyber tools and tradecraft, disclosing them to the public, and, when necessary, using offensive cyber operations to prevent adversary threats. The apparent success of the Defend Forward strategy in negating threats to the 2018 and 2020 US elections suggests that this more proactive approach is likely to be sustained in some form and perhaps expanded in the future. However, Defend Forward will need to be adapted to allow improved defense at home because, as evidenced in both the 2020 SolarWinds and the 2021 Microsoft Exchange hacks, cyber adversaries are increasingly launching intrusions from US territory.

On a day-to-day basis, below the level of armed conflict, the NCDC would plan and coordinate a sustained cyber defense campaign across the US government, including enabling appropriate coordination with the private sector, state and local governments, and key allies and partners.

To more effectively counter adversary cyber campaigns and protect American interests, the United States should expand the Defend Forward strategy in five ways: from focusing overseas to also actively defending much better at home; from being DoD-centric to integrating all key government departments and agencies; from building a few US industry and international partnerships for "hunt forward" efforts and information sharing to creating and sustaining scores of such relationships at home and abroad; from a focus on election security to also addressing other challenges, including countering the theft of intellectual property, countering disinformation campaigns, and preventing massive compromises that expose US critical infrastructure to disruption or destruction; and from an event-focused episodic effort to a long-term national cyber defense campaign.

What an NCDC Would Do

Operating as an element of the ONCD under presidential guidance and oversight from the National Security Council (NSC), the NCDC would conduct long-term campaign planning to guide a whole-of-government effort and would coordinate the exercise of cyber defense authorities from all relevant federal departments and agencies. It would further aim to enable a whole-of-nation effort by prioritizing US government intelligence sharing and cyber defense coordination with key private sector partners and state and local governments. The center would also prioritize and coordinate cyber defense efforts with key allies and partners.

In addition to planning and coordinating the day-to-day battles in cyberspace conducted below the level of armed conflict, the NCDC would conduct contingency planning and if necessary coordinate cyber defense of the United States in the event of a conflict.

Cyber Defense below and above the Level of Armed Conflict

On a day-to-day basis, below the level of armed conflict, the NCDC would **plan and coordinate a sustained cyber defense campaign** across the US government, including enabling appropriate coordination with the private sector, state and local governments, and key allies and partners. This cyber defense campaign would focus particular attention on China and Russia—the two great power competitors, and most capable cyber adversaries, of the United States. It would also address North Korea, Iran, ISIS, and other cyber adversaries.

In addition to planning and coordinating the day-to-day battles in cyberspace conducted below the level of armed conflict, the NCDC would **conduct contingency planning and if necessary coordinate cyber defense of the United States in the event of a conflict**. This role would be particularly important in a crisis or conflict with China or Russia, both because of their advanced cyber capabilities and because of the severe risks inherent in any great power war. In addition to targeting military networks and systems, adversaries could attack US civilian critical infrastructure through cyberspace with disruptive impact on both military operations and civilian life. Achieving a rapid and coordinated US cyber defense effort could be of critical importance in a conflict; moreover, if the United States is perceived to have this ability, it could make a vital contribution to deterrence of armed aggression.

NCDC Key Lines of Effort and Objectives

The NCDC would plan and coordinate four interrelated lines of US cyber defense: cyber deterrence, active cyber defense, offensive cyber actions in support of defense, and incident management. For each of these lines of effort, the NCDC would aim to help the United States achieve specific outcomes with respect to specific cyber adversaries, as outlined below.

Cyber deterrence aims to reduce adversaries' perceived benefits and increase the perceived costs and risks of major cyber intrusions, attacks, or cyber-enabled campaigns, such as China's theft of intellectual property and Russia's efforts to sow domestic discord in the United States. Because of the extensive vulnerabilities of existing US networks, deterrence by denial will not be adequate against advanced adversaries, particularly China and Russia. Deterrence by cost imposition (i.e., the threat of retaliation) will be essential; this requires intelligence-driven planning to help policymakers assess what responses may be strong enough to promote deterrence but not so strong as to lead to undesired escalation. Although the US government has sometimes retaliated in response to cyber attacks (e.g., with diplomatic expulsions, economic sanctions, and legal actions), to date it has not planned or conducted a systematic cyber deterrence campaign effort. Defining and defending norms of appropriate behavior in cyberspace below the level of armed conflict, and creating international support for these norms, will be an important element of such a deterrence campaign effort.

Cyber deterrence objective: The cyber adversary chooses not to intrude or attack, or desists from an ongoing campaign, because it is deterred or accedes to cyber norms and associated international pressure.

Active cyber defense starts from the understanding that advanced adversaries, China and Russia in particular, have substantial resources and highly skilled teams that will allow them to penetrate US networks and systems (even those with much-improved passive cyber defenses) through a variety of techniques. Active cyber defense aims to rapidly detect and mitigate intrusions, increase the attacker's "work factor" (time and resources required to achieve its aims by expanding laterally, exfiltrating information, etc.), and reduce the attacker's confidence that intrusions have succeeded and that any information extracted is accurate. Examples of active cyber defense tactics include "hunting" for cyber intrusions on one's own (and partners') networks, creating "honeypots" and "tarpits" to lure and trap cyber intruders in decoy servers, embedding false information on networks that may mislead intruders, and publicly releasing insights into adversary cyber tools and tradecraft. Active cyber defense is increasingly being conducted by both the US government and the private sector but not in a comprehensive, coordinated campaign approach. There is much room for improved sharing of operationally relevant (timely and specific) information, intelligence, and insights.

Active cyber defense objective: The cyber adversary is forced to expend large amounts of resources (funding and scarce time of talented hackers) because of the high "work factor" and is uncertain whether it has succeeded or whether information extracted is accurate; in addition, cyber deterrence is strengthened because the United States is more prepared to thwart cyber intrusions and attacks against its society, economy, and military.

Offensive cyber actions in support of cyber defense can be both necessary and appropriate, as exemplified by US Cyber Command's reported operations to thwart the Russian Internet Research Agency troll farm in the 2018 and 2020 US elections. Careful planning and close coordination among US departments and agencies is essential and a campaign approach would be beneficial for a number of reasons: the necessity to trade off potential losses of intelligence; the requirement for consistent communication to the adversary as well as to allies; the potential to either support or undermine proposed norms of conduct in cyberspace; the likelihood that the cyber adversary will operate from US territory as well as overseas; and (particularly for China and Russia) the potential for escalation. By all public accounts, US Cyber Command's actions in support of the 2018 and 2020 US elections were carefully considered and well-coordinated across the US government; however, as the scope of such operations below the level of armed conflict increases and/or if the United States finds itself in a crisis or conflict with China or Russia, a whole-of-government campaign approach will be essential to provide well-considered courses of action as well as well-practiced processes for swift, whole-of-government decision-making.

The NCDC must ensure that the US government works effectively with key actors in the private sector in developing, implementing, and over time adapting cyber campaign plans.

Objective for offensive cyber operations in support of cyber defense: The cyber adversary is blocked from achieving its aims without the United States extensively undermining desired norms of cyber conduct or inadvertently causing escalation; in addition, cyber deterrence is strengthened because the United States is more capable of preventing costly cyber intrusions and cyber attacks against its society, economy, and military.

Cyber incident response will always remain a key part of US cyber defense efforts because neither passive cyber defense efforts nor the other three key lines of NCDC operations will fully succeed in all cases against the most capable adversaries. Unlike the other lines of effort proposed for the NCDC, there currently exists a well-rehearsed interagency process for cyber incident response. Because cyber incident response is so intertwined with the other NCDC lines of effort, it makes sense to shift the oversight of interagency Cyber Unified Coordination Groups (which are established to coordinate US government responses to major cyber incidents) to the NCDC. In parallel, the NSC would shift its focus from operational coordination to strategic decision-making and oversight, including prioritizing US government support in the event of widespread cyber intrusions or attacks and holding the NCDC and the ONCD accountable for conducting its operational role.

Cyber incident response objective: In the event of a major cyber intrusion or attack, the integrity and availability of US critical infrastructure is rapidly restored so that the adversary is unable to achieve its aims and US interests are protected; in addition, cyber deterrence is strengthened because the United States is more prepared to mitigate serious cyber intrusions and crippling cyber attacks against its society, economy, and military.

The value of a whole-of-government, long-term campaign approach to planning and coordination is clear when one considers each of the above lines of effort—and that most or all of them would need to be conducted in parallel and could either reinforce or undermine each other.

Bolstering Private–Public Partnerships

To protect privacy and civil liberties, the private sector must take the lead in protecting its critical assets in cyberspace. Given this reality, the private sector, and not the US government, will have the essential knowledge regarding what is occurring within networks and systems in the event of crisis or conflict. This means that the US government must play a supporting role in taking actions within the United States to defend privately owned critical infrastructure.

The NCDC must ensure that the US government works effectively with key actors in the private sector in developing, implementing, and over time adapting cyber campaign plans. Although unclassified campaign planning would be of great value for raising the overall level of cyber defense in the United States, some planning and coordination efforts may involve sensitive intelligence regarding the adversary. In such cases involving sensitive intelligence, it would be reasonable to involve only the largest companies that account for a major share of the US economy. Sharing highly sensitive intelligence with key communication service

providers, cloud service providers, and cybersecurity companies could allow them to modify their services to help a large number of private sector companies, citizens, and the US government.

A key role of the NCDC would be to identify barriers to effective and timely private–public partnerships and advocate for changes in the US government necessary to improve the overall cyber defense posture of the United States. Today's system is not set up for operating at the speed of relevance in crisis or conflict, and as a result, in a great power crisis or conflict, there would almost certainly be avoidable failures to "connect the dots" (or avoidable errors in rushing to judgment and incorrectly connecting dots) and to take action in a timely manner.

A continuous net assessment process for cyberspace can be thought of as an ongoing simulation of strategic interactions in cyberspace between the United States and each competitor/adversary (and other relevant players).

Engaging State and Local Governments and US Allies/Partners

The NCDC must have strong connectivity with US states and localities to coordinate cyber efforts, including law enforcement and National Guard support. As seen in other national disaster response activities, large cities can be on the front lines and can often provide the earliest warnings that an attack is underway. One component of the NCDC, perhaps led by a senior Department of Homeland Security (DHS) person with a Federal Bureau of Investigation (FBI) deputy and connected closely to DHS's Cybersecurity and Infrastructure Security Agency (CISA), would be responsible for bringing state and local governments appropriately into the planning process and engaging them in operational coordination. Such planning and coordination could also be facilitated by creating secure collaboration capabilities between state cyber "expert centers" and the NCDC.

The engagement of key US allies and partners in the US government's cyber defense efforts is essential both to improving the defense of US networks and to deterring aggression overseas. The NCDC would be responsible for coordinating and proposing priorities for such engagements across domestic, defense, and intelligence agencies. One early objective for an NCDC might be to increase the coordinated activities of "like-minded" nations and entities.

Key Supporting Function: A Continuous Net Assessment Process

It would be unrealistic to expect effective planning or coordinated government and private sector action to occur day to day or in crisis/conflict in the absence of a shared common perspective of the current situation and an ability to share a visualization of potential future developments. Sustaining a shared common perspective requires creating and maintaining a platform for securely sharing data and analytical insights within the US government and with select private sector partners, at appropriate classification levels. Sharing a visualization of potential future developments requires, additionally, a gaming/simulation platform for conducting (human and machine) simulations and analyses aiming to anticipate the most likely and most dangerous future adversary courses of actions—including responses to actions that the United States might take.

Providing shared perspectives on the current situation and potential future developments, through tailored visualization tools based on a wide range of data sources, would be a key role of the NCDC. Such a continuous net assessment process would not be able to "predict" precisely what the adversary will do, but over time—and with continued reality testing—the US ability to anticipate potential adversary courses of action should improve. A continuous net assessment process for cyberspace can be thought of as an ongoing simulation of strategic interactions in cyberspace between the United States and each competitor/adversary (and other relevant players).

This process would be supported by intelligence/counterintelligence assessments and informed by tabletop war gaming, modeling and simulation, and results from cyber range activities. The objective is not only to assess the current situation but also to assist intelligence analysts, planners, and decision-makers in anticipating potential future adversary courses of action, alternative US options, and how those actions and options may interact with each other and with other key actors' choices.

Such a net assessment process would help highlight areas where additional information and intelligence are most needed. Because adversaries are adapting as they exploit emerging cyber vulnerabilities, this net assessment process could also generate testable hypotheses regarding next adversary moves so that intelligence assets can be directed appropriately, defensive measures can be taken, and offensive measures can be preplanned. To counter adapting adversaries, this net assessment process must exploit new technologies, such as artificial intelligence and machine learning.

The NCDC could achieve an initial operating capability with fewer than one hundred personnel, perhaps with as few as thirty to forty.

NCDC Organizational Structure and Staffing

An NCDC would be an integral part of the congressionally mandated ONCD. The organizational structure of the NCDC could, and probably should, evolve over time. From the outset, its organization should be based on a few key principles.

- The **director** should be a senior civilian with both senior-level US government and private sector experience as well as the confidence of the National Cyber Director and the deputy national security advisor for cyber and emerging technology.
- The **vice director** should also be an experienced leader, with complementary expertise and background, and would likely be either active duty, reservist, or a member of the National Guard.
- **Deputy directors** should, as a group, have experience across all key departments and agencies, including the Departments of Homeland Security, Defense, State, and Treasury as well as various elements of the Intelligence Community.
- To ensure a continued focus on cyber adversaries, critical planning and coordination activities should take place in "**country cells**" (China, Russia, etc.), and the staffing for each would be drawn from multiple departments and agencies.

- Because the NCDC would be an extraordinarily lucrative target for cyber espionage and attack, it would need a **top-notch chief information officer and chief information security officer** and would need to exemplify as well as enable a diverse set of advanced tools and techniques for active cyber defense.
- All offices (generally under deputy directors) should be organized not by department/agency but by function, with each having an interagency composition and with each being composed significantly of **detailees** from key departments and agencies.

The NCDC would not displace department and agency cyber centers, but would coordinate their work. Federal cyber centers, such as the FBI's National Cyber Investigative Joint Task Force and DHS's CISA Central, would continue their work while supporting planning and coordinated campaigns orchestrated by the NCDC. Similarly, the Intelligence Community's Cyber Threat Intelligence Integration Center would see the NCDC as a critically important customer; even as it continued to provide strategic intelligence to the NSC, it would build its capacity to provide operationally relevant and timely intelligence to the NCDC.

The NCDC could achieve an initial operating capability with fewer than one hundred personnel, perhaps with as few as thirty to forty. Although the enabling legislation for the ONCD caps total personnel at seventy-five, the legislation specifically allows the office to "utilize, with their consent, the services, personnel, and facilities of other Federal agencies."[1] Thus, for example, a one-hundred-person NCDC that was 60 percent detailees would count only against forty of the allowed seventy-five ONCD slots. Such a model makes good sense in any event: to effectively integrate the authorities of various departments and agencies, the NCDC should be composed mostly of detailees from key departments and agencies.

The NCDC's interagency staff would conduct planning, coordinate already-approved interagency actions, and raise new proposals and any concerns regarding department/agency noncompliance with the NSC.

In order to succeed over time, the NCDC will need to compete successfully for its share of talented cyber professionals. Given the importance of this national center, the president might direct department and agency heads to provide their best personnel to field an all-American cyber defense "dream team" and could further make a personal appeal to industry CEOs. Over the course of a decade or so, after there had been five or more rotations of detailed/assigned personnel from the US government and private sector, an informal network within the federal government and between it and the private sector will have been established. If over this period the NCDC averaged seventy personnel with fifty being rotational, there could be a cadre of 250 or more highly trained, experienced, and networked personnel who had rotated through the NCDC.

This reality creates an important opportunity for the NCDC to serve as a flywheel for interagency and national-level training and education on cyber defense (including, in particular, experiential learning through exercises and real-world operations). An enlightened NCDC leadership would work to maximize this benefit through training and education efforts and the encouragement of continued professional relationships among those who had served in the NCDC.

[1] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395.

How an NCDC Would Operate

The NCDC's interagency staff would conduct planning, coordinate already-approved interagency actions, and raise new proposals and any concerns regarding department/agency noncompliance with the NSC. Such actions would be administratively straightforward.

The NCDC director would request approval for new activities from the department(s) or agency head(s) with the requisite authorities, simultaneously sending the request to the NSC's deputy national security advisor for cyber and emerging threats for interagency consideration. The deputy national security advisor would have the prerogative—and the responsibility—to determine whether to call for NSC meetings, and if so, with what urgency and at what level (full NSC chaired by the president, Principals Committee chaired by the national security advisor, Deputies Committee chaired by the deputy national security advisor, or a supporting interagency working group).

For extremely time-urgent decisions, department and agency heads could approve execution before interagency consideration; in this case, an operation could be initiated even as NSC consideration was beginning. The relevant department or agency head would be accountable to the president for justifying their choice to proceed. In cases that involved both time urgency and a very good understanding of escalation risks, over time this decision authority could be delegated further, with the objective of having the vast majority of actions taken by department and agency heads or their subordinates, with concurrent notification of the NSC staff. Of course, at any time the president may direct the execution, or nonexecution, of a proposed new activity.

What an NCDC Would Not Do

An NCDC would fill a current gap in US government organization and processes relating to cyber defense by integrating department and agency cyber defense operations (including supporting information and intelligence) through campaign planning and operational coordination. It is also important to note what it would not do.

- The NCDC would not set strategic direction for the nation; this would remain the job of the president and NSC. NCDC planning would be conducted under presidential guidance and reviewed in an NSC process; its operational coordination would be subject to NSC oversight while respecting the authorities of department and agency heads.
- The NCDC would not have "command and control" authority over department and agency heads or supplant the need for them to build capacity. Indeed, the NCDC's success would depend on departments and agencies continuing to exercise their authorities and build cyber expertise and increased capacity to fulfill their roles.
- The NCDC would not (1) direct operations (the president, or appropriate department and agency heads, would do so); (2) conduct operations (departments and agencies would do so); (3) plan or coordinate cyber operations not related to national cyber defense (e.g., military cyber operations aimed at supporting regional combatant commanders); or (4) plan or oversee passive cybersecurity standards or the development of more defensible cyber architectures and components.

Organizational Placement and Physical Location

The NCDC would not fit in the NSC, quite literally, given the legislative staffing cap of two hundred NSC personnel. Even if the cap were increased, the NSC staff should be focused on coordinating and overseeing the implementation of strategy and policy, not conducting ongoing campaign planning and coordinating operations. Placing the NCDC in DHS's CISA, or in another department or agency, would be a prescription for failure. Developing and coordinating the execution of national campaign and contingency plans for cyber defense—plans that really matter—will require departments and agencies to share sensitive intelligence and operational capabilities; a standing interagency body in the Executive Office of the President is needed to make this work. In addition, there is the question of seniority: an NCDC director reporting to the CISA director would sit two levels below the Deputies Committee, whereas an NCDC director reporting to the (principal-level) NCD would operate at the deputies level. Anyone with experience working in the US interagency process understands how important these differences of organizational placement and seniority of the NCDC director would be in practice.

Even with the best virtual collaboration and planning tools, planning and coordination works best when done face-to-face.

This reality raises a bit of a conundrum: In the same defense authorization bill that created the ONCD, Congress mandated the creation of a Joint Cyber Planning Office (JCPO) in CISA with the mission of developing plans for cyber defense operations. Congress might in principle be persuaded to reverse itself, but there is another viable option: the director of the JCPO could be dual-hatted as the lead for private sector and state/local government engagement in the NCDC. Wearing the CISA "hat," this person could make use of all DHS authorities as JCPO director; wearing the NCDC "hat," this person could also influence others beyond the reach of DHS authorities, including national security departments and agencies as well as US allies and partners.

Even with the best virtual collaboration and planning tools, planning and coordination works best when done face-to-face. Thus, it will be essential to have a cadre of interagency personnel and private sector liaisons who work under the same roof to plan, coordinate, and build mutual knowledge and trust. Because senior members of the NCDC would need to meet with key department/agency leaders and attend NSC meetings on a regular basis, the NCDC should be located either in or within short driving distance of Washington, DC. Because the NCDC would be an extremely attractive target for foreign espionage, it should be located in a highly secure facility with the best-in-government physical security and cybersecurity. To establish the NCDC without having to wait for a new building construction, it should be placed in a location that has immediately available secure space and some ability to grow. Placing the NCDC at Ft. Meade would meet all these criteria; alternative locations in the Washington, DC, area (if available) would allow a shorter trip to the White House Situation Room and key departments.

Setting a Course for Success

An NCDC would bolster the US strategic position in cyberspace, especially relative to great power competitors China and Russia, which appear to be increasing both the scope of their cyber intrusions

and their use of US-based infrastructure as a platform for their attacks. It would provide a major step function increase in the US government's ability to take a long-term campaign approach that integrates the spectrum of interagency authorities and capabilities necessary to cyber defense.

Establishing an NCDC offers the potential for a major improvement in the US posture in cyberspace.

An NCDC can provide improved day-to-day integration of national efforts across departments and agencies, faster and higher-confidence national decision-making regarding cyber, and thoughtful contingency planning that will reduce risks of inadvertent escalation while bolstering deterrence. Like all organizations, an NCDC will have growing pains and will make mistakes; the goal should be for an NCDC to advance to a mature organization within two years, after it has made most of its mistakes in war games and simulations rather than in the real world.

Establishing an NCDC offers the potential for a major improvement in the US posture in cyberspace. Put differently, if an NCDC existed today and functioned reasonably well in its planning and operational coordination missions, and in its net assessment function, any proposal for its elimination would be seen clearly to leave a major gap in the ability of the US government to compete in cyberspace below the level of armed conflict, and if necessary, to fight and manage escalation in cyberspace. That gap exists today and is evident to US competitors and adversaries, thus putting US national security at avoidable risk.

This report examines the establishment of a National Cyber Defense Center (NCDC), which would plan and coordinate US cyber defense operations below the threshold of armed conflict while also conducting contingency planning and if necessary coordinating cyber defense operations in the event of armed conflict. The NCDC would be embedded within the congressionally mandated Office of the National Cyber Director (ONCD) and would work under the guidance of the National Security Council (NSC).

The NCDC would aim to achieve a whole-of-government cyber defense effort by leading campaign planning and coordinating the exercise of authorities from all relevant federal departments and agencies. This center would aim to bring a coherent and consistent approach to four key lines of effort: cyber deterrence; active cyber defense effort with the private sector and international partners (including information and intelligence sharing as well as coordinated actions); where necessary, offensive cyber operations in support of cyber defense; and national cyber incident response.[2] As an integral part of each line of effort, the center would coordinate and propose how to further enable and empower US government (USG) partnerships on cybersecurity with the private sector, state and local officials, and key allies and partners.

The remainder of this report proceeds as follows. After briefly describing the most pressing cyber threats facing the United States, we explain how in recent years US cyber strategy has shifted toward active cyber defense and the use of offensive cyber operations to deter, thwart, or respond to cyber attacks. Next, we sketch the missions and organizational structure of an NCDC, describe how its cyber defense planning and coordination might contribute both below the level of armed conflict and in a great power crisis/war, and assess its potential costs, risks, and benefits. A key issue that we address is how the prerogatives of departments and agencies could be maintained, including the role of the Department of Homeland Security (DHS) in national cybersecurity, the prerogatives of the Intelligence Community, the leadership role of the Federal Bureau of Investigation (FBI) and Justice Department in investigating cyber crime and cyber terrorism, and the secretary of defense's and US Cyber Command commander's roles in the military chain of command. We then consider how such a center might be established and sustained and assess alternative transition strategies. We conclude with recommendations for creating and growing an NCDC in order to give it the best possible prospects for success.

The stakes in this ongoing cyber competition below the level of armed conflict include the health of US democracy, social cohesion, and America's technological advantage.

Cyber Threats to US National Security

USG and private sector networks are subjected to intrusion and attack by state and nonstate actors on a daily basis. In some cases, these actors seek to cause disruption (e.g., North Korea's attack on Sony Entertainment in 2014), and in other cases, they seek to advance objectives ranging from conducting espionage, to stealing intellectual property, to sowing social discord. In the event of a crisis or conflict, particularly with China or Russia, early moves by each side in cyberspace could rapidly escalate to broad and punishing attacks on civilian critical infrastructure. As noted below, cyber threats to US national security below and above the threshold of armed conflict are linked closely, and it is important that the USG conduct

[2] A good description of active defense is provided in GWU CCHS, *Into the Gray Zone.*

integrated planning and coordination to address them both.

Cyber Threats below the Level of Armed Conflict

The United States is engaged in a day-to-day, high-stakes battle in cyberspace, which plays out below the threshold of armed conflict. State and nonstate actors are exploiting the open architecture and distributed defenses of US digital infrastructure to garner sensitive information and intelligence, steal intellectual property, spread disinformation to sow domestic division, employ ransomware for financial gain, and conduct cyber attacks to advance their political agendas.

The stakes in this ongoing cyber competition below the level of armed conflict include the health of US democracy, social cohesion, and America's technological advantage, all of which undergird the United States' military edge and economic growth. Because US allies and partners are also being subjected to such cyber and cyber-enabled attacks, their stability and security are also at risk, with significant implications for US national interests.

Both state and nonstate adversaries are conducting sustained cyber-enabled campaigns against the United States. Cyber crime, including ransomware, is estimated to account for a loss of more than 1 percent of US gross domestic product (GDP) annually.[3] Cyber ransomware attacks targeting the health care industry have disrupted hospitals and put patients at risk.[4] With the rapid growth of the Internet of Things, the attack surface for cyber criminals is growing dramatically.

Although disruptive one-off cyber attacks such as North Korea's attack on Sony Entertainment in 2014 garner much public attention, long-term campaigns conducted by China and Russia in particular may pose much greater risks to the US economy and political system. China and Russia have both engaged in extensive (and reportedly highly successful) cyber espionage, stealing designs of emerging military systems, personal information about US citizens, and even insights into the development of a vaccine for the novel coronavirus.[5] China's cyber-enabled theft of intellectual property has been estimated to cost the United States 1–2 percent of GDP annually and has been described as "the greatest transfer of wealth in human history."[6] The FBI reported that, as of February 2020, it had more than one thousand ongoing investigations relating to Chinese cyber theft.[7]

The failure to stem cyber espionage and associated malware implants has resulted in an erosion of US military advantage and incalculable risks to American security.

The fabric of American society and the US political system are also under attack in cyberspace, as a number of countries, particularly Russia but also including China and Iran, are conducting cyber-enabled disinformation attacks to sow domestic discord and undermine democracy in the United States. Russia's interference in the 2016 US presidential election and continued purveying of

[3] The global costs of cybercrime are estimated to be approaching $1 trillion per year. See Smith, Lostri, and Lewis, *Hidden Costs of Cybercrime*.

[4] See CISA, "Alert (AA20-302A)." See also Smart, *Lessons Learned Review*.

[5] Barnes and Venutolo-Mantovani, "Race for Coronavirus Vaccine."

[6] The Commission on the Theft of American Intellectual Property estimated that in 2017, "the annual cost to the U.S. economy continues to exceed $225 billion in counterfeit goods, pirated software, and theft of trade secrets and could be as high as $600 billion." Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report*. See also Commission on the Theft of American Intellectual Property, *IP Commission 2019 Review.*

[7] *Guardian*, "China Theft of Technology."

online disinformation has been well documented by US intelligence agencies and described by the Senate Intelligence Committee as "a calculated and brazen assault on the United States and its democratic institutions."[8] China and Iran reportedly joined Russia in using cyberspace to conduct influence operations on the American public during the 2020 election cycle.[9] The challenge of disinformation in an age of ubiquitous social media is daunting, in part because, as noted by former DHS Cybersecurity and Infrastructure Security Agency (CISA) director Chris Krebs, "our democratic institutions are facing targeted, calculated threats from without, and from within."[10] If the United States does not stanch the flow of this ongoing bleed of sensitive information and diminution of citizen/ally confidence, the nation will be substantially weakened over time.

The failure to stem cyber espionage and associated malware implants has resulted in an erosion of US military advantage and incalculable risks to American security.[11] The massive SolarWinds hack—uncovered in 2020 and attributed to the Russian Foreign Intelligence Service—may have exposed thousands of USG and private sector networks and systems to espionage and potentially disruption. The also massive Microsoft Exchange hack—discovered in 2021 and attributed by Microsoft to China—has been reported to have left tens of thousands of organizations exposed.[12] As noted by Microsoft President Brad Smith, these intrusions were "effectively an attack on the United States and its government and other critical institutions, including security firms."[13]

As discussed in the next section of this report, the United States has adapted its cyber strategy in recent years to focus more on preventing cyber intrusions and cyber attacks below the level of armed conflict. Yet trends appear adverse.[14] A particular concern is that cyber intruders and attackers can operate not only from within their own country but also from within other countries, including US allies and indeed the United States, a challenge highlighted by the massive SolarWinds and Microsoft Exchange cyber intrusions.[15]

In addition to the challenges posed by China and Russia, other actors, including North Korea and Iran, terrorists, and criminal groups, have significant and growing cyber intrusion and attack capabilities. Although these other actors do not have the sophistication or capacity of China or Russia, they have the ability to undermine US foreign policy goals, impose significant harm through cyber attacks, and complicate timely attribution, any of which could confuse or delay US decision-making in a major power crisis.

In the event of a severe crisis or conflict, China and Russia could use cyber weapons to hobble the US military, cripple the US economy, and sabotage systems that deliver life-critical services.

For example, North Korea is estimated to have stolen nearly $2 billion from banks and cryptocurrency

[8] SSCI, *Report on Russian Active Measures*.

[9] See Owens, *60 Minutes*. See also ODNI, "Statement by NCSC Director."

[10] Krebs, "We Prepared for More Russian Interference."

[11] Among the known losses to cyber espionage was critical information on the F-35 Joint Strike Fighter. See Gallagher, "Australian Defense Firm Was Hacked."

[12] Krebs, "At Least 30,000 U.S. Organizations."

[13] Smith, "Moment of Reckoning."

[14] For a summary of major cyber incidents since 2006, see CSIS, "Significant Cyber Incidents."

[15] An article on SolarWinds noted that "hackers managed their intrusion from servers inside the United States, exploiting legal prohibitions on the National Security Agency from engaging in domestic surveillance and eluding cyberdefenses deployed by the Department of Homeland Security." Sanger, Perlroth, and Barnes, "As Understanding of Russian Hacking Grows." See also Lyngaas, "CISA Orders US Agencies."

accounts to fund its illicit weapons programs.[16] North Korea was also responsible for the 2017 WannaCry 2.0 attacks and the 2014 attack on Sony Entertainment.[17] Since conducting distributed denial-of-service (DDoS) attacks on Wall Street in 2012–2013 and hacking the Sands Casino in 2014, Iranian cyber threat actors "have continuously improved their offensive cyber capabilities" and "have also demonstrated a willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks."[18]

While stealing billions of dollars per year, cyber criminals have worked to mask their identities. For example, starting in 2019, one group posed as highly capable Russian state-sponsored hackers as they extorted businesses by threatening large-scale DDoS attacks if substantial ransoms in cryptocurrency were not paid.[19] This real-world, ongoing challenge serves as a caution that criminals, terrorists, or third-party nations could pose as Chinese or Russian state-sponsored hackers in the midst of a severe crisis with the United States, raising the prospect of one side taking countervailing action in cyberspace and possibly dramatically escalating a conflict.

Cyber Attacks in Crisis or Conflict

In addition to posing daily challenges of cyber competition below the threshold of armed conflict, China and Russia have extensively infiltrated US critical infrastructure with implanted cyber capabilities on a scale and at a level of sophistication that far exceed those of any other potential US adversaries.[20] Of particular concern, both China and Russia have reportedly gained footholds in the information technology systems supporting the US electrical grid.[21]

The ability to rapidly conduct coordinated active defense of critical networks and systems in the early days of a great power conflict could make an enormous contribution to the resilience of the US economy and society, and the ability of US armed forces to conduct operations effectively.

In the event of a severe crisis or conflict, China and Russia could use cyber weapons to hobble the US military, cripple the US economy, and sabotage systems that deliver life-critical services—all while conducting all-out cyber-enabled disinformation and deception efforts in an attempt to sow discord among the American people.[22] If the United

[16] *BBC News,* "North Korea 'Stole $2bn.'"

[17] CISA, "Alert (AA20-106A)."

[18] CISA, "Alert (AA20-006A)."

[19] Cimpanu, "DDoS Gang Is Extorting Businesses."

[20] Coats, *Statement for the Record*.

[21] The DoD's 2020 annual report on China concluded that "China is improving its cyberattack capabilities and has the ability to launch cyberattacks—such as disruption of a natural gas pipeline for days to weeks—in the United States." OSD, *Military and Security Developments*, 83. A 2018 joint DHS and FBI report concluded: "Since at least March 2016, Russian government cyber actors—hereafter referred to as 'threat actors'—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors." CISA, "Alert (TA18-074A)." A 2020 report by the NSA noted that "one of the greatest threats to U.S. National Security Systems (NSS), the U.S. Defense Industrial Base (DIB), and Department of Defense (DoD) information networks is Chinese state-sponsored malicious cyber activity. These networks often undergo a full array of tactics and techniques used by Chinese state-sponsored cyber actors to exploit computer networks of interest that hold sensitive intellectual property, economic, political, and military information." NSA, "Chinese State-Sponsored Actors."

[22] A recent article on Russian views noted that "Russia is implementing policies and practices designed to promote information warfare to a level of parity with nuclear and conventional power." Tashev, Purcell, and McLaughlin, "Russia's Information Warfare."

States does not posture itself better to be able to prevent and rapidly remediate such cyber attacks conducted on (and from) American infrastructure, US deterrence of coercion or armed aggression will be undermined.

A 2017 Defense Science Board (DSB) study concluded that "the unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures."[23] Unfortunately, despite efforts to reduce the vulnerability of US critical infrastructure, there have been no significant, systemic changes in critical infrastructure defense since the DSB report of 2017, and the United States remains vulnerable to debilitating cyber attacks by China or Russia. The ability to rapidly conduct coordinated active defense of critical networks and systems in the early days of a great power conflict could make an enormous contribution to the resilience of the US economy and society, and the ability of US armed forces to conduct operations effectively.

The vulnerability of US critical infrastructure to large-scale cyber attack by another great power creates a broader set of strategic vulnerabilities. China or Russia could use offensive cyber capabilities, including cyber-enabled disinformation operations and identity exploitation operations, to adversely impact national security in a number of ways. For example, such operations could delay the deployment and impair the use of US armed forces in support of allies and partners, allowing China or Russia to achieve a fait accompli and to put the burden of escalation to reverse their military aggression on the United States; deter American intervention in support of allies and partners by holding at risk US civilian critical infrastructure; or attempt to coerce the United States in matters of diplomacy or trade relations through the capacity to impose sustained pain on the US economy.

These possibilities are not lost on Chinese or Russian leaders, who are working to improve their cyber offensive capabilities and deepen their penetrations of US critical infrastructure. The Pentagon's 2020 report on China's military power concluded that "Chinese writings suggest cyber operations allow China to manage the escalation of a conflict because cyber attacks are a low-cost deterrent. The writings also suggest that cyber attacks demonstrate capabilities and resolve to an adversary."[24] A recent Office of the Director of National Intelligence (ODNI) threat assessment notes similar intent on the part of the Russian Federation: "Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat."[25]

The risks associated with high-impact Chinese or Russian cyber attacks on US critical infrastructure in the context of a crisis or war may not seem as pressing as daily cyber intrusions and attacks. However, the current situation poses serious strategic risks for the United States, as the vulnerabilities of US armed forces and society to cyber attacks undermine both the military capabilities and political credibility of US commitments to defend its allies and partners from armed aggression.

Linkages between Cyber Threats above and below the Threshold of Armed Conflict

Cyber challenges above and below the threshold of armed conflict are intertwined in three essential ways. First, day-to-day US cyber operations below the threshold of armed conflict affect the likelihood that a great power crisis or conflict will occur. On

[23] DoD, *Task Force on Cyber Deterrence*, 4.

[24] OSD, *Military and Security Developments*, 74–83.

[25] Coats, *Statement for the Record*.

one hand, an overly passive US approach could invite adversaries to keep pushing out the limits until US leaders finally feel compelled to respond with decisive force. On the other hand, an overly aggressive approach by the United States could cause a spiral of escalation. A well-calibrated approach in peacetime, based on an assessment of adversary interests and goals and an explicit assessment of escalation risks, is needed to minimize the prospects of both failed deterrence and inadvertent war. Although the lines between peace, crisis, and war can appear to be blurred when cyberspace is involved, it nonetheless must remain a key US priority to both deter and avoid stumbling into war with China or Russia.

Second, the Clausewitzian "fog" and "friction" of daily cyber engagements would carry over and indeed be amplified in the event of a great power crisis or conflict. Because third-party nations could conduct cyber attacks that were initially assessed to come from China or Russia, US policymakers would quite sensibly require high-confidence attribution (i.e., wait for the fog to clear) before responding; this delay might prevent us from stumbling into war, or it might undermine deterrence of aggression and so increase the prospects of great power war. In addition, the challenges inherent in the American government coordinating its actions internally and with the private sector (i.e., friction among US actors that can slow responses and make them less coherent) and potentially allies on a day-to-day basis would likely be exacerbated in the environment of a high-stakes, time-constrained great power crisis. Moreover, the recognition of these realities creates opportunities for China and Russia to exploit. For example, China or Russia might obfuscate its role in early cyber attacks in order to achieve an advantage before the United States has achieved definitive attribution. Alternatively, China or Russia could enlist second-tier nations such as North Korea or Iran, or increasingly powerful and more agile cyber-criminal groups, to undertake (or just provide a platform for) cyber attacks on the United States. The reality that fog and friction are present in cyberspace means that US decision-making in the shadow of a great power conflict must account for third-party actors such as North Korea and Iran, and do so in a confident and timely manner. Both the conduct of daily cyber operations and the planning and preparation for actions in crisis or conflict must account for these realities.

At the advent of the internet age in the 1980s, little thought was given to defending the small but rapidly growing network of connected computers.

Third, US cyber activities in peacetime provide the essential foundation for cyber operations in crisis or conflict. The organizations, planning, processes, capabilities, and trust relationships needed for an effective active cyber defense of US critical infrastructure, rapid decision-making for any offensive cyber operations, and cyber incident management in the event of great power conflict cannot be created instantaneously when a crisis arises; they must be developed, exercised, and matured in peacetime if they are to be available in the event of crisis or conflict. Moreover, even if such capabilities could be magically established in a crisis, the lack of such capabilities in peacetime could very well contribute to the failure of deterrence or the poorly considered actions that can lead to crisis in the first place. In a very real sense, US peacetime cyber activities—including true private–public partnerships allowing near real-time sharing of sensitive information—and coordination of actions provide a "platform" for cyber operations in crisis and conflict, and adversary perceptions of these capabilities in action can help to reduce the risk of great power war.

US Cyber Defense Strategy

This section provides a brief overview of US cyber strategy. It concludes that US cyber strategy has evolved to include four key elements in addition to "passive defense" that require an integrated whole-of-government approach to succeed: cyber deterrence, active cyber defense, offensive cyber actions in support of cyber defense, and cyber incident management. Appendix A provides more extensive historical details regarding the evolution of US cyber strategy.

At the advent of the internet age in the 1980s, little thought was given to defending the small but rapidly growing network of connected computers. This changed in November 1988, when the Morris worm disrupted an estimated six thousand of the eighty-eight thousand computers (many USG-owned) then connected to the nascent internet.[26] Although the damage from the Morris worm was limited, the risk of future disruption was recognized. Two cyber defense–related initiatives resulted.

First, new efforts were undertaken to reduce the vulnerabilities of computers and networks through "computer network defense"—what would today be described as ***passive cyber defense***. These measures include, for example, the use of more complex passwords, firewalls, timely software updates, and personnel training. Such passive defense measures remain foundational to any cyber defense strategy.[27]

In part because many of the computers initially connected to the emerging internet until the mid-1990s were government-owned or supported USG research, the initial focus of US cyber strategy was to reduce the vulnerabilities of telecommunications and information technology that directly supported national security departments and agencies. By the late 1990s, as recognition grew that the essential services provided by privately owned US critical infrastructure were also vulnerable to cyber disruption, US cyber strategy broadened to attempt to address the vulnerabilities of key privately owned systems, while still focusing on passive cyber defense.

By the late 1990s and early 2000s, as serious cyber intrusions and attacks below the level of armed conflict mounted, it became clear that the cyber vulnerabilities of both government and privately owned critical infrastructure were likely to remain for many years. Although improvements in passive cyber defense were still rightly viewed as necessary (to minimize cyber crime and cyber terrorism and to increase the resources state actors have to apply to penetrate critical US networks), passive defenses were clearly not sufficient. Over time it became increasingly clear that given the capabilities of advanced adversaries, in particular China and Russia, a strategy based solely on passive defense was certain to fail.

Second, in parallel with efforts to bolster passive cyber defenses, the USG began to develop capabilities for (what today would be called) ***cyber incident response***. Indeed, within a few months of the Morris worm incident in 1988, the Defense Advanced Research Projects Agency (DARPA), which had sponsored the development of the Arpanet, funded and established the first-ever Computer Emergency Response Team (CERT) at Carnegie Mellon University.[28] Over the following decades, both the USG and private sector

[26] Holohan, "As the Morris Worm Turned."

[27] The SANS Institute has crafted a definition based on the protective nature of passive defenses that describes passive cyber defense as "systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction." Lee, *Sliding Scale of Cyber Security.*

[28] Now known as the Computer Emergency Response Team Coordination Center (CERT/CC). CERT/CC is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University. Since 2003, SEI has also hosted the separate US-CERT, which, under sponsorship from the Department of Homeland Security, serves as the national computer security incident response team. See https://www.sei.cmu.edu/about/divisions/cert/.

companies have increased their capabilities for cyber incident response.

As cyber intrusions and attacks grew, US policymakers were, for understandable reasons, unsatisfied with a strategy based solely on passive cyber defense and cyber incident response. Such a strategy appeared to cede all initiative to adversaries and allow them to achieve their aims at very limited cost and little risk.

Building private–public and international partnerships is central to the active defense model.

Thus, during the George W. Bush administration, US cyber strategy added a new element: ***cyber deterrence***, which in principle aimed to reduce the benefits and increase the costs to an adversary for cyber intrusions, cyber attacks, and cyber-enabled campaigns.[29] Although deterrence was now part of the stated strategy, there were no publicly known cost-imposing responses to cyber intrusions on the United States, as the national security establishment was focused predominantly on ongoing wars in Afghanistan and Iraq.

During the Obama administration, cyber strategy continued to evolve. An extensive Russian intrusion into both unclassified and classified Department of Defense (DoD) networks drove the new Obama administration to stand up a new US Cyber Command, publish a new cyber defense strategy predicated on active cyber defense, and launch a new *International Strategy for Cyberspace* that promulgated the right of the United States to respond in kind to cyber attacks.[30] On a number of occasions, including in response to Iran's 2012–2013 DDoS attack on Wall Street and North Korea's 2014 hack of Sony Entertainment, the Obama administration imposed costs on cyber attackers through diplomatic, economic, and law enforcement actions.

In addition, the Obama administration took additional steps to establish supporting norms of appropriate cyber conduct—for example, a 2012 presidential agreement with China to refrain from cyber-enabled theft of intellectual property. Although Chinese cyber-enabled theft of intellectual property was reported to decline somewhat for a period, in this instance and others, efforts to establish and enforce norms did not appear to have a sustained impact on cyber intrusions.

By 2017, many observers concluded that the United States was not effectively deterring attacks below the level of armed conflict. A new US cyber defense strategy, first articulated in early 2018 in US Cyber Command's new vision statement[31] and subsequently reiterated in DoD and national strategy documents, represented a marked shift. As noted by US Cyber Commander General Paul Nakasone, the objectives of the "Defend Forward" strategy were to "generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere."[32] In addition to threatening cyber retaliation in response to cyber attacks, the new strategy emphasized two new elements in addition to incident response and cyber deterrence.[33]

Beyond passive cyber defense, ***active cyber defense***, aims to minimize the scope and severity of cyber intrusions by fighting back, principally within

[29] White House, *National Strategy to Secure Cyberspace*.

[30] DoD, *Department of Defense Strategy*; and White House, *International Strategy for Cyberspace*.

[31] USCYBERCOM, *Achieve and Maintain Cyberspace Superiority*.

[32] *Hearing on the Fiscal Year 2021 Budget Request*, statement of General Paul M. Nakasone.

[33] Per the author's communication with then-deputy assistant secretary of defense for cyber policy Ed Wilson, the Russian cyber attacks on the Democratic National Committee network in 2016 helped to drive a consensus in USG to take the next steps with active cyber defense, including indictments and the Defend Forward strategy.

one's own networks and systems. It aims to detect cyber intrusions quickly through intelligence and "hunting" on one's own networks to increase the attacker's "work factor" (time and resources required to achieve its aims by expanding laterally, exfiltrating information, etc.) and to reduce the attacker's confidence that their intrusions have succeeded and that any information extracted is accurate. Active defense efforts include disseminating information on adversary cyber tools and tradecraft gleaned to help government, private sector, and allied/partner nations better protect themselves.[34]

Building private–public and international partnerships is central to the active defense model. In 2018, US Cyber Command deployed personnel to Montenegro, North Macedonia, and Ukraine in its "hunt forward" effort, partnering with DHS and the FBI to release malware publicly.[35] In 2020, US Cyber Command's efforts expanded to include (at least) Estonia.[36] Based on this cooperative effort and less than a week before the 2020 elections, the press reported that US Cyber Command "uploaded samples of the new ComRAT and Zebrocy versions on its VirusTotal account, while CISA, in cooperation with the FBI's CyWatch, published two security advisories describing ComRAT and Zebrocy's inner workings."[37]

Such cooperative efforts, including the public release of malware signatures, also reinforces cyber deterrence efforts, both by reducing the benefits of an intrusion and increasing its (reputational and actual) costs. As noted by the Estonian Defense Forces' Cyber Command's Deputy Head Mihkel Tikk: "If we discover the malicious activity and we share it with the world, our partners, then attacking is more expensive. So the adversary has to start making decisions and making choices about who they attack."[38]

The third key element beyond passive cyber defense involves the use of ***offensive cyber operations*** to thwart serious cyber intrusions, cyber attacks, or cyber-enabled campaigns (e.g., to steal intellectual property or conduct disinformation). Although such actions have been a stated part of US cyber strategy since 2011[39] and offensive cyber operations were used against al-Qaeda and ISIS, no publicly known preemptive cyber actions were taken against nation-states until 2018, when the USG shifted to the more proactive approach of Defend Forward.

Although some questioned whether the new Defend Forward strategy would work and others feared it might result in escalation,[40] to date the results of applying this new strategy in the 2018 and 2020 US elections appear extremely promising. Substantial foreign interference in US elections appears to have been prevented, with no apparent signs of serious escalation risks. This is an especially impressive achievement given the time constraints in 2018 (the Russia Small Group effort began in earnest only weeks before the election) and the much larger scope of the Election Security Group's efforts in 2020 (USG efforts had to expand to counter not only Russian but also Chinese and Iranian cyber-enabled information operations).[41]

The success of the Defend Forward strategy in negating threats to the 2018 and 2020 US elections suggests that this approach is likely to be sustained and expanded in the future to address a broader range of cyber threats; for example, this strategy

[34] As US Cyber Commander General Nakasone later noted, "We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts." Lopez, "Cyber Command Expects Lessons."

[35] Vavra, "Cyber Command Deploys Abroad."

[36] USCYBERCOM, "Hunt Forward Estonia."

[37] Cimpanu, "US Cyber Command Exposes."

[38] Barnes, "U.S. Cyberforce Was Deployed to Estonia."

[39] Alexander, "US Reserves Right."

[40] Healey, "Implications of Persistent (and Permanent) Engagement."

[41] See Barnes, "U.S. Cyber Command Expands Operations." See also Starks, "Russia, China and Iran."

might be used to protect sensitive information and intellectual property, counter malign disinformation and propaganda campaigns, and deter or prevent cyber attacks against US and allied/partner critical infrastructure.

If so, the next essential evolution will be to move toward a stronger integration of all tools of national power in an integrated whole-of-government effort to establish more effective cyber deterrence, enhance active defense, and set conditions for broad international support for preemptive, offensive cyber actions when needed. ***Cyber incident response*** will still be essential, of course, because the combination of cyber deterrence, active defense, and preemption will sometimes fail to prevent cyber intrusions and attacks; at the same time, continuing active defense during a cyber incident will be essential. Moreover, close coordination between incident response and active cyber defense in particular is critical because a key part of the response should be to engage in (and bolster) active cyber defense. Moreover, incident response and active cyber defense are likely to rely on an overlapping group of cyber experts and involve engaging the same government and private sector organizations that have been victimized by intrusion or attack.[42]

In March 2020, US Cyber Commander General Nakasone offered a remarkably detailed statement in open testimony to Congress that shed new light on Defend Forward actions in 2018 and plans for the 2020 elections:

> Last year, we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond. The group reports directly to me and is led by representatives from Cyber Command and the National Security Agency. Its objectives are to generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere. To be sure, we place a high priority on collecting and sharing information with our partners at DHS and FBI to enable their efforts as part of a whole-of-government approach to election security. But Cyber Command's authorities mean that it must also be prepared to act.
>
> In 2018, these actions helped disrupt plans to undermine our elections. During multiple "hunt forward" missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.
>
> Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.[43]

The 2020 Cyberspace Solarium Commission report offered an in-depth assessment of the US cyber posture, with many of its recommendations

[42] Incident response is predicated on three activities working in parallel: (1) ongoing damage assessment; (2) active pursuit of the perpetrator; and (3) how and when to remediate in light of no. 1 and no. 2.

[43] *Hearing on the Fiscal Year 2021 Budget Request*, statement of General Paul M. Nakasone.

put into law in the fiscal year 2021 National Defense Authorization Act (NDAA). Its first and highest-level recommendation regarded strategy:

> First, the executive branch should issue a new national cyber strategy bringing coherence to the federal government's efforts. That strategy should be based on this Commission's framework of layered cyber deterrence, emphasize resilience and public-private collaboration, build on the Department of Defense's (DoD) concept of defend forward as a government-wide effort, and prioritize a bias for action.[44]

For the remainder of this report, we assume that the USG will follow a cyber strategy broadly along the lines suggested by the commission. This strategy would continue to work to build inherently more secure critical infrastructure and bolster passive defenses over the long term; such efforts are critical but would not be the focus of an NCDC.

An updated US national cyber defense strategy would expand from Defend Forward in five ways:

- from focusing overseas to also actively defending much better at home;
- from being DoD-centric to integrating all key government departments and agencies;
- from building a few US industry and international partnerships for "hunt forward" efforts and information sharing to creating and sustaining scores of such relationships;
- from a focus on election security to also addressing other challenges, including countering the theft of intellectual property and countering disinformation campaigns; and
- from an event-focused episodic effort to a long-term national cyber defense campaign, which includes contingency planning to prepare for crisis or conflict.

Planning and coordinating such an expanded cyber defense campaign would be the focus of an NCDC.

What an NCDC Would Do

An NCDC would have two interrelated missions, which are discussed in detail below: (1) to conduct campaign planning and day-to-day operational coordination for cyber defense below the level of armed conflict and (2) to conduct contingency planning and operational coordination of cyber defense in crisis or conflict. It would make use of all key departments' and agencies' cyber defense–relevant authorities, capabilities, and interagency activities in its planning and operational coordination. And, as discussed below, the NCDC's planning and coordination efforts would prioritize and leverage engagement of the private sector, state and local governments, and key international partners.

In support of all its efforts, it would be essential for the NCDC to implement a continuous net assessment process, described in detail below, to inform the planning and adaptation of ongoing operations. Because future adversaries are likely to undertake cyber attacks from within the US homeland as well as from overseas, a key aspect of the NCDC's assessment process would involve integrating domestic information and foreign intelligence.

NCDC Mission 1: Conduct campaign planning and coordination of US cyber defense below the threshold of armed conflict.

The NCDC would develop and coordinate the execution of an integrated interagency cyber defense campaign plan aimed at reducing the incidence and impact of significant cyber intrusions,

[44] CSC, *CSC Report*, 31.

cyber attacks, and cyber-enabled influence operations against the United States and allies.

In order to do so, the NCDC would adopt a systematic campaign approach that is proactive rather than reactive; that integrates offensive, defensive, and intelligence actions in cyberspace; and that incorporates all elements of national power, including cyber defense–related diplomacy, law enforcement, economic, intelligence, military, and strategic communications. To be proactive and to adapt quickly to new developments, a cadre of personnel from key departments/agencies—including (at least) the Departments of Homeland Security, Defense, State, Commerce, Treasury, Energy, and Justice (particularly the FBI), the Central Intelligence Agency (CIA), and the broader Intelligence Community—must work together on a day-to-day basis. This group constitutes the minimal core members of an NCDC.

If US allies and partners support cyber norms, they are likely to be more willing to support imposing costs on violators, thus substantially improving the credibility, severity (through multilateral cost imposition), and sustainability of US threats to impose costs in response to violations.

To plan and coordinate campaign efforts from day to day, the senior leaders of the NCDC must have visibility into directly related activities, including ongoing or planned offensive cyber operations and covert action, if any. The NCDC must also have a good understanding of the status of partnerships with owners of critical infrastructure in the private sector as well as with key allies and other partners.

Operating under guidance from the president and oversight from the NSC, the NCDC would conduct strategic planning and operational coordination in support of four key lines of effort:

- ***deterring cyber attack*** on the United States and its allies, in part by imposing costs on violators of norms of appropriate behavior in cyberspace;
- conducting ***active cyber defense*** to increase the attacker's "work factor" and to reduce the attacker's confidence that intrusions have succeeded and that any information extracted is accurate;
- when necessary using ***offensive cyber operations in support of cyber defense***, such as those US Cyber Command reportedly conducted against the Russian Internet Research Agency troll farm in defending the 2018 and 2020 US elections; and
- when the preceding efforts are inadequate and significant cyber intrusions and attacks occur, ensuring the coordination of USG efforts to conduct and support national ***cyber incident response***.

Cyber Deterrence

Cyber deterrence aims to reduce cyber attacks by affecting the decision calculus of adversaries. As noted by the congressionally mandated Cyberspace Solarium Commission: "The central idea is simple: increase the costs and decrease the benefits that adversaries anticipate when planning cyberattacks against American interests."[45] In recent years, the USG has imposed a range of penalties on state actors in response to cyber attacks and cyber-enabled attacks, including diplomatic expulsions, the imposition of economic sanctions, and legal actions. However, the USG to date has not planned or conducted a cyber deterrence campaign effort that sets priorities and integrates all tools of national power.

[45] CSC, *CSC Report*, 24.

Although the concept of cyber deterrence is straightforward, the challenge of deterring costly cyber intrusions or attacks below the level of armed conflict is significant. In particular, deterring China or Russia by decreasing their benefits is challenging because they (like the United States) have sophisticated and well-funded cyber programs with substantial resources. At the same time, deterring them by cost imposition is challenging because the benefits of cyber intrusions (e.g., gaining economic advantage through the theft of intellectual property) are often quite high, and US leaders may be reluctant to impose punishing costs especially given the vulnerability of US critical infrastructure to cyber attack.

Notwithstanding these challenges, there is little question that the United States could do better in deterring cyber attack (and avoiding inadvertent escalation) if it developed and executed a campaign plan based on best assessments of adversary goals and values as well as estimates of likely responses to US actions. As noted in a 2017 DSB report on cyber deterrence:

> A campaign perspective is needed in order to better deter future attacks, to avoid underreacting or over-reacting to specific incidents, and to drive the prioritization of both defensive and offensive capabilities. It is essential that cyber deterrence planning not focus only on one-off events (such as a large-scale attack on civilian critical infrastructure), but be formulated as a campaign that is continuous. In one sense, the United States has a campaign underway today to deter cyber attacks—but to date, that campaign has been largely reactive and not effective.[46]

The USG has supported the establishment of norms or "rules of the road" for cyberspace. Although the USG has attempted to develop international consensus on norms in cyberspace through such initiatives as the Group of Government Experts, a UN-sanctioned, multiyear activity to achieve such international support, this effort and other like efforts have not been successful, primarily because of the objections of US adversaries such as China and Russia.[47] China and Russia have proposed other ideas for driving cyberspace "rules of the road." Their work has been focused on developing alternative standards and the associated architecture for use of cyberspace—architecture and rules that are counter to US and allied values supporting an open and secure internet.[48] Getting China and Russia to agree to follow some set of international norms—aligned with the open and secure use of the internet—would bolster deterrence to some degree; as Joseph Nye has noted, a nation's adherence to norms "can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack."[49]

The value of norms in directly affecting adversary behavior is limited at best, as suggested by the fact that both China and Russia have a significant history of violating norms and codes of conduct to which they have subscribed, such as China's commitment not to steal US intellectual property and Russia's claim to support noninterference in the domestic affairs of other nations. However, norms have a second, and perhaps more important, impact on deterrence: if US allies and partners support cyber norms, they are likely to be more willing to support imposing costs on violators, thus substantially improving the credibility, severity (through multilateral cost imposition), and sustainability of US threats to impose costs in response to violations. A good example of where such progress has been made is in the area of cyber crime with the ratification of the Budapest Convention in 2003. Since then, sixty-five nations, including the United

[46] DoD, *Task Force on Cyber Deterrence*, 11.

[47] Henriksen, "End of the Road."

[48] Murgia and Gross, "Inside China's Controversial Mission."

[49] Nye, "Deterrence and Dissuasion in Cyberspace," 60.

States, have become signatories to this multilateral agreement. Importantly, national law enforcement agencies are now working together and with Interpol to forge new enforcement mechanisms for countering cyber crime beyond their national borders.[50] That being the case, much more needs to be done and could be done to improve cyber deterrence through the formation of a more expansive International Cyber Stability Board of like-minded nations.[51]

An effective cyber deterrence effort will require systematic planning that evaluates what the adversary leadership is aiming to achieve and what it values—and then considers how best to deny its objectives or impose meaningful costs. Similarly, strengthening norms of appropriate cyber behavior will require a careful consideration of not only what the United States and its allies will do in response to cyber intrusions and attacks, but what they will refrain from doing in support of cyber norms.

Cyber deterrence aims to achieve this strategic objective:

The cyber adversary chooses not to intrude or attack, or desists from an ongoing campaign, because it is deterred and/or accedes to cyber norms and associated international pressure.

Active Cyber Defense

Active cyber defense starts from the understanding that although capable cyber intruders, particularly China and Russia, will gain a foothold in many key public and private networks and systems, that does not mean the battle is over. Active cyber defense aims to detect and mitigate intrusions, increase the attacker's "work factor" (time and resources required to achieve its aims by expanding laterally, exfiltrating information, etc.), and reduce the attacker's confidence that intrusions have succeeded and that any information extracted is accurate.

Although the USG and private sector have taken a number of steps in recent years to improve the cybersecurity and cyber resilience of critical government systems and civilian critical infrastructure, even under the best of circumstances, building much more cyber-secure and resilient systems is a long-term and uncertain proposition. The conclusion reached by the DSB in 2017 remains true as of 2021:

> The unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures.[52]

In recognition of the reality that boosting cyber resilience is necessary but not sufficient, both the private sector and USG have engaged increasingly in active cyber defense in recent years.[53] Whereas passive defense involves measures such as the use of firewalls, antivirus software, and software updates, active cyber defense involves activities ranging from "hunting" for intrusions on one's own networks, to attempting to deceive and hinder attackers (e.g., by using "honeypots" to attract them to less valuable data and systems and "tarpits" to attempt to prevent them from moving laterally), to botnet takedowns conducted by the private sector.

One example of active cyber defense is the public release of information about malware, such as that by DHS, the FBI, the National Security Agency (NSA), and US Cyber Command during election defense efforts in 2018 and 2020; of note, some of these releases involved leveraging US Cyber Command's "hunt forward" efforts in Montenegro,

[50] Council of Europe, *Budapest Convention on Cybercrime.*

[51] Kramer, Butler, and Lotrionte, "Raising the Drawbridge."

[52] DoD, *Task Force on Cyber Deterrence*, 4.

[53] Rosenzweig, Bucci, and Inserra, *Next Steps for U.S. Cybersecurity.*

North Macedonia, and Ukraine (in 2018) and in Estonia (in 2020). Another recent example of active cyber defense occurred in October 2020, when Microsoft (reportedly with some USG support) took legal action to take down infrastructure facilitating the Trickbot botnet.[54]

Active cyber defense is especially important in mitigating advanced cyber intrusions and attacks, and private–public partnerships are especially important to effective active cyber defense. As noted by one government agency, "the ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling unity of effort in successfully detecting and defending against advanced cyber-attacks."[55] Active cyber defense is increasingly being conducted by both the USG and the private sector but typically not in a comprehensive or coordinated fashion. There is much room for improved sharing of operationally relevant (timely and specific) information, intelligence, and insights.

Active cyber defense aims to achieve this strategic objective:

The cyber adversary is forced to expend large amounts of resources (funding and the scarce time of talented hackers) because of the high "work factor" and is uncertain whether it has succeeded and/or whether information extracted is accurate; in addition, cyber deterrence is strengthened because the United States is more prepared to thwart cyber intrusions and attacks against its society, economy, and military.

Offensive Cyber Actions in Support of Cyber Defense

Offensive cyber operations may be needed in some cases to prevent a serious cyber intrusion, cyber attack, or cyber-enabled attack from occurring. The most notable known examples to date of such cyber actions are US Cyber Command's efforts to take down infrastructure supporting the cyber-enabled influence operations by Russia and others during the 2018 and 2020 US elections, including its disruption of the Russian Internet Research Agency's troll farms.[56] It is worth highlighting that in these cases, offensive cyber actions were taken along with efforts to conduct active cyber defense (as outlined above).

An NCDC would also propose offensive cyber actions in support of cyber defense—that is, offensive cyber operations by the USG to prevent or thwart cyber intrusions and attacks. In conducting its planning, the NCDC would essentially provide a "demand signal" for US Cyber Command (and the CIA if covert action were authorized) to plan and, if directed, conduct offensive cyber operations in support of cyber defense of the United States. In conducting its coordination role, the NCDC would work to integrate such actions into a broader interagency effort that would include (for example) active cyber defense, diplomacy, and strategic communications.

It is important to note that the US Congress confirmed in 2018 that such offensive cyber actions conducted in self-defense represent a legitimate use of military force below the level of armed conflict. US private sector companies are not allowed to conduct preemptive cyber defense (or any form of offensive cyber operations such as "hacking back") under US law and so must depend on the USG to conduct such actions when necessary. Because of the potential for escalation, careful planning and

[54] Burt, "New Action to Combat Ransomware." This Microsoft post states, "We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world. We have now cut off key infrastructure so those operating Trickbot will no longer be able to initiate new infections or activate ransomware already dropped into computer systems."

[55] NSA, "Active Cyber Defense."

[56] *Hearing on the Fiscal Year 2021 Budget Request*, statement of General Paul M. Nakasone.

close coordination are essential.[57] Under Title 10 of the US Code, US Cyber Command has authority to undertake offensive cyber actions, as a part of traditional military activities, to defend US interests below (and above) the threshold of armed conflict. Under Title 50, the CIA (or another agency) could undertake offensive cyber actions, which in principle could include supporting cyber defense, to achieve the aims of a presidential finding.

The Justice Department has important authorities allowing it (and in particular the FBI) to facilitate investigations,[58] but it is important to note that federal, state, and local governments do not have the authority to undertake offensive cyber operations within the United States. As a result, private–public partnerships—ranging from "tipping and cueing" (e.g., the government providing information to private sector companies to help them eradicate specific threats on their networks) to conducting coordinated "takedowns" of adversary infrastructure domestically and overseas—are critically important to the protection of US critical infrastructure.

With the NCDC in place, the USG would have be better postured to respond both more quickly and more appropriately to major cyber intrusions.

Careful planning and coordination are clearly needed for offensive cyber operations in support of cyber defense. These offensive cyber operations will require extensive preparation, and it will be essential to continuously assess whether they tend to reinforce deterrence and desired norms of conduct in cyberspace and/or whether they carry any substantial risks of escalation.

Offensive cyber actions in support of cyber defense aim to achieve this strategic objective:

The cyber adversary is blocked from achieving its aims without any extensive undermining of the desired norms of cyber conduct or inadvertent escalation; in addition, cyber deterrence is strengthened because the United States is more capable of preventing costly cyber intrusions and cyber attacks against its society, economy, and military.

Cyber Incident Response

As noted in the previous section, interagency USG processes for cyber incident response exist today and have been exercised multiple times.[59] For example, in response to the SolarWinds intrusions discovered in late 2020, the FBI, CISA, and ODNI formed a Cyber Unified Coordination Group to coordinate their respective relevant activities as well as to leverage other USG capabilities.[60] Each element of the federal government was responsible

[57] See, for example, Schmidle, "Digital Vigilantes."

[58] For example, consider the following from the Justice Department: "To circumvent the challenges presented by threat actors' use of proxies and Tor, investigators can use Network Investigative Techniques ('NITs'). NITs include computer code that investigators can send covertly to a device that is hidden behind proxies. Once installed, a NIT can send law enforcement particular information, often including the device's true IP address—which investigators then can use to identify the subscriber and user of the device." Cyber-Digital Task Force, *Report of the Attorney General's Cyber Digital Task Force*, 54.

[59] The White House's *Presidential Policy Directive* states that a significant cyber incident "is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

[60] As noted earlier, Cyber Unified Coordination Groups "serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate." White House, *Presidential Policy Directive*.

for exercising its authorities as well as for supporting other departments and agencies. For example, the FBI was responsible for "engaging with known and suspected victims, and information gained through FBI's efforts will provide indicators to network defenders and intelligence to our government partners to enable further action."[61]

It would be difficult to overstate the importance, or the challenge, of cyber defense of the United States in the context of a great power armed conflict.

Such interagency processes would remain in place with the establishment of an NCDC, with the NCDC being responsible for establishing and overseeing the responses of interagency Cyber Unified Coordination Groups to significant cyber incidents. The NCDC would immediately set the US response in the context of current campaign plans for the relevant country (in the case of SolarWinds, reportedly Russia); propose steps that not only respond to the cyber intrusion but attempt to reestablish cyber deterrence and make use of active cyber defense measures (e.g., "hunting" on USG networks, tailoring "tarpits" to help prevent lateral movement by the intruder, and supporting the private sector as well as allies and partners' efforts to take similar actions); and propose offensive cyber actions that could blunt the ongoing cyber intrusion or impose costs on the national leadership directing this intrusion.

With the NCDC in place, the USG would be better postured to respond both more quickly and more appropriately to major cyber intrusions. It is likely that some proposals by the NCDC would require senior policymakers' consideration of whether they would advance US interests, be supported by allies and partners, be consistent with efforts to establish cyber norms, and so on. Such questions would need to be addressed in the NSC process, which would continue to give guidance and provide oversight of cyber incident response. The NSC would focus on strategic decisions and would hold the NCDC and the national cyber director accountable for planning and coordinating a whole-of-government approach to cyber defense.

It is critical to make the NCDC responsible for coordinating interagency cyber incident response efforts for four reasons. First, cyber incident management is tightly intertwined with the other three lines of NCDC effort; for example, reinforcing cyber deterrence and conducting active cyber defense would be high priorities for the USG in the event of a major cyber incident, and it is possible that offensive cyber actions would be considered to prevent further attacks and/or impose costs on the attacker. Second, there is a limited supply of people in the USG with cyber expertise and strong networks in the private sector, and it would be inefficient to divide them up between those focused on (in particular) active cyber defense and incident response. Third, private sector owners of critical infrastructure should not have to deal with multiple USG agencies with overlapping agendas that are not coordinated, especially in the event of a major cyber incident in which incident response and attempts to improve active cyber defense and deterrence would be deeply intertwined. Fourth, and not of least importance, the NCDC staff (including department and agency detailees) will gain experience and insight through involvement in cyber incident response, which will help give them the information, judgment, and contacts necessary to better perform their deterrence and active cyber defense efforts.

[61] CISA, "Joint Statement."

Cyber incident response aims to achieve this strategic objective:

In the event of a major cyber intrusion or attack, the integrity and availability of US critical infrastructure is rapidly restored so that the adversary is unable to achieve its aims and US interests are protected; in addition, cyber deterrence is strengthened because the United States is more prepared to mitigate serious cyber intrusions and crippling cyber attacks against its society, economy, and military.

NCDC Mission 2: Conduct cyber defense contingency planning and coordination.

The NCDC would develop cyber defense contingency plans, and in the event of crisis or conflict, provide operational coordination between elements of the USG responsible for the defense of domestic and overseas digital infrastructure, the collection and analysis of relevant domestic information and foreign intelligence, and engagement with key private sector, state and local, and international partners.

It would be difficult to overstate the importance, or the challenge, of cyber defense of the United States in the context of a great power armed conflict. China and Russia are using advanced cyber intrusion tools to gain access to US critical infrastructure, and the United States is reported to be taking similar actions.[62] In the event of armed conflict, each side would have strong incentives to undertake early, impactful cyber attacks to hobble the other side's military or demonstrate the ability to impose costs through cyber attacks on civilian critical infrastructure. Such early cyber attacks could provide military and coercive advantage without a shot ever being fired outside of cyberspace.[63]

Thus, in addition to planning and coordinating the day-to-day battles in cyberspace conducted below the level of armed conflict, the NCDC would plan and if necessary coordinate cyber defense of the United States in the event of a conflict. National cyber defense contingency planning would contribute to US national security in at least four overlapping ways.

Preparing for and Conducting Coordinated Cyber Defense in Crisis or Conflict

First, and most obviously, cyber defense contingency planning would prepare the United States to conduct a coordinated and more effective cyber defense (including supporting intelligence collection and analysis) in the event of a great power conflict. In such a scenario, both the United States and its adversary would have strong incentives to attack early and extensively in cyberspace to delay and degrade the other side's military, and to signal the potential to inflict economic and social pain.

From the perspective of the president and US policymakers, there would be major risks associated with either doing too little or doing too much during a crisis to take down potential adversary cyber threats. And there could be intense time pressure to decide.

Preparatory contingency planning would include development of indicators and warnings of a cyber attack on the United States (differentiating between scenarios such as escalation in cyberspace versus

[62] Sanger and Perlroth, "U.S. Escalates Online Attacks"; and Barnes, "U.S. Cyber Command Expands Operations."

[63] In keeping with traditional Soviet notions of battling constant threats from abroad and within, Moscow perceives the struggle within "information space" to be more or less constant and unending. This suggests that the Kremlin will have a relatively low bar for employing cyber in ways that US decision-makers are likely to view as offensive and escalatory in nature. Connell and Vogler, *Russia's Approach to Cyber Warfare.*

a broader crisis involving aggression against US allies), creation of cyber defense alert and readiness levels, and development of an emergency playbook of interagency cyber defense options. These options would span all four areas of the NCDC's scope: how to bolster or attempt to reinstate **deterrence** (including potential actions and statements to signal resolve, a desire for de-escalation, etc., and to bolster allies' cyber posture); new measures that could be taken to enhance or adapt **active cyber defenses** (e.g., deploying teams to support expanded "hunting" on US and allied networks, conducting preplanned changes to the configurations of select networks and systems, working with the private sector to take down adversary-controlled infrastructure); if directed by the president, actively blunting adversary cyber capabilities through **offensive cyber operations**; and conducting **cyber incident response**, likely at a scale never before seen. Such contingency planning would need to be tested and refined through red teaming, war games, and simulations and would aim to improve the odds of taking the right actions at the right time.

Prioritizing Engagement with Key Partners

Second, the United States would far prefer to deter a great power conflict than to fight one; the NCDC could plan and implement, as part of a broader interagency plan, efforts to bolster deterrence of great power coercion or attack. Actual preparedness to defeat or impose costs in response to aggression is the starting point of an effective deterrence posture, which must also signal both capability and commitment to the adversary.

The NCDC contingency planning effort should consider how to signal capabilities and resolve to Chinese and Russian intelligence, military commanders, and political leaders. As one example, contingency planning might suggest actions that the United States could take to show that it has an increasingly effective active cyber defense capability. As a second example, the planning effort might consider how to deceive potential adversaries regarding true vulnerabilities that have not been mitigated.

Identifying Escalation Risks That Could Arise in Day-to-Day Execution of Campaign Plans

Third, by exploring possible pathways to great power conflict, contingency planning would help to identify offensive cyber or (in principle) other actions that the United States or allies might consider in peacetime but should be held in reserve to deter or prosecute conflict. Such actions might be preserved because they are most relevant to deterrence or to war-fighting or because it is judged that China or Russia would be likely to interpret them as an act of war. Through such analysis, the NCDC may contribute both to strengthened deterrence and to reducing the risk of inadvertent war.

Concerns about deterrence of armed aggression, and crisis stability, should inform the planning and coordination of day-to-day cyber operations below the level of armed conflict. The actions that the United States takes in the day-to-day competition must be calibrated to be neither too little (thereby weakening deterrence and encouraging more adversary cyber aggression below the level of armed conflict) nor too much (thereby inadvertently causing unwanted escalation).

Prioritizing Key Private Sector and International Partner Engagements

Fourth, in the event of great power conflict, cyber attacks would likely arise not only (or likely even predominantly) from the adversary's territory, but also (as seen in the 2020 SolarWinds and 2021 Microsoft Exchange hacks) from within US territory as well as the territory of key allies and

partners. Similarly, cyber attacks from multiple (and often obfuscated) locations would likely occur against US and ally/partner infrastructure overseas. Dealing effectively with these challenges will require integrated planning and coordinated cyber defense operations within the United States and with key allies and partners.

Thus, some private sector companies and international partners will be more important than others for sustaining US cyber defense capabilities in the event of a conflict. Others may be prioritized for cyber defense because of their contribution to sustaining critical functions ranging from military operations (e.g., transportation companies critical to deployment of forces and allies essential to the hosting of US forces) to continuity of government and continuity of the economy. A systematic NCDC contingency planning process would identify these priority partners so that the United States would be prepared to rapidly prioritize engagement with them.

To protect privacy and civil liberties, the private sector must take the lead in protecting its critical assets in cyberspace.

Enabling Key Partnerships for Cyber Defense

The NCDC will not succeed without expanding and deepening current USG relationships with the private sector. In addition, strong relationships with US state and local authorities and US allies and partners will be important. Moreover, the NCDC must both leverage and help accelerate the creation of an interagency cross-trained cadre with expertise in planning and operations, as well as rapid innovation and the fielding of new capabilities.

Engaging the Private Sector

In addition to the challenge of integrating the capabilities and authorities of government departments and agencies, there is a gap today in domestic operational capacity. The USG can collect intelligence and conduct cyber operations overseas, including through the CIA, the NSA, and US Cyber Command, but for good reasons, including the Fourth Amendment's protection against unreasonable searches and seizures as well as broader public expectations of privacy and civil liberties, it lacks an analogous capability domestically absent appropriate court approvals. Yet an effective national cyber operational capability must account for attacks occurring both on and from privately owned domestic infrastructure. USG cyber experts will not be able to provide timely intelligence or assistance to the private sector if the first engagement is in the midst of a major attack.

To protect privacy and civil liberties, the private sector must take the lead in protecting its critical assets in cyberspace.[64] Given this reality (at least) in peacetime, the private sector, and not the government, will have the essential knowledge regarding what is occurring within networks and systems in the event of crisis or conflict. This means that the USG must play a supporting role in taking actions within the United States to defend privately owned critical infrastructure.

[64] Many private sector owners of critical infrastructure, particularly in the financial sector, have invested substantially in protecting their data, hardening their networks, and bolstering cyber resiliency. A study by Deloitte found that in 2020, the typical US financial firm was spending nearly $2,700 per full-time employee on cybersecurity, with financial utilities (which provide the infrastructure necessary for conducting financial transactions) averaging $4,375 per full-time employee. Bernard and Nicholson, "Reshaping the Cybersecurity Landscape." As explained by the Federal Reserve Board, "Financial market utilities (FMUs) are multilateral systems that provide the infrastructure for transferring, clearing, and settling payments, securities, and other financial transactions among financial institutions or between financial institutions and the system." Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities."

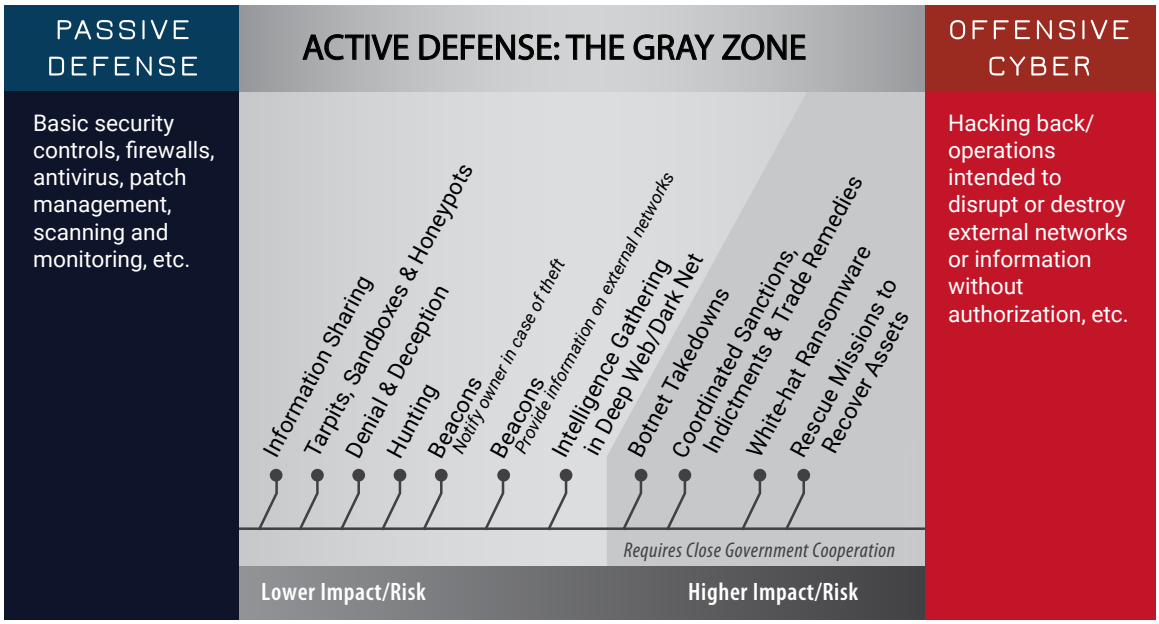
The NCDC must work closely with the private sector in developing, implementing, and over time adapting cyber campaign plans. Some aspects of the planning effort can be unclassified and so engage hundreds or thousands of private sector entities. However, some elements of the campaign planning and implementation will involve highly sensitive information and/or highly sensitive operations and so must involve only a relatively small number of private sector firms with cleared personnel and the ability to manage sensitive compartmented information.

As an initial starting point, it would be reasonable to involve in the most sensitive campaign planning and implementation only the largest American telecommunications providers (e.g., AT&T, Verizon, CenturyLink), the largest American cloud computing providers (e.g., Microsoft, Amazon, Google, IBM), and the largest providers of active cyber defense capabilities. The infrastructure that these companies provide affects a significant fraction of the US economy, and most or all these companies have substantial staffs skilled in a range of active cyber defense activities, including intelligence collection and hunting on their own networks. Only a handful of personnel in each of these companies would require access to highly sensitive compartmented information in order to participate; because cyber-related decisions could affect companies' profitability and even viability, executive leadership (CEOs, CFOs, COOs) as well as CIOs and Chief Information Security Officers (CISOs) should be among those with such clearances.

Since at least the 1997 Marsh Commission Report, the federal government has recognized the importance of private–public collaboration on cybersecurity. Over time, this collaboration has become ever more important as adversary cyber capabilities improve and as private sector companies pursue active cyber defense in the "gray zone." The gray zone is generally regarded as the region on the spectrum of competition and conflict that lies between peace and war; although the gray zone spans all domains (for example, the term covers China's use of "white hull" Coast Guard ships to control maritime lanes in the South China Sea and Russia's use of "little green men" to occupy eastern Ukraine), much of global gray zone activities occur in cyberspace, and the United States must compete more effectively in this zone to protect its national interests.

Private–public collaboration is particularly important in conducting active cyber defense. Figure 1 offers a private sector view of active cyber defense—more than passive defense but less than offensive cyber operations. The range of activities shown in Figure 1 suggests at least three important implications for private–public partnerships on cyber defense:

- First, the USG can help enable private sector active defense operations by sharing timely information and intelligence and by coordinating USG actions with private sector actions in a coordinated way. Many large private sector companies now have the technical wherewithal, knowledge, and authorities to thwart adversary attacks through active defense. Figure 1 shows the wide range of activities that this may entail, from information sharing (within the industry, with the government, or publicly), to employing denial and deception regarding network and system vulnerabilities, to hunting on their own (or clients') networks, to "taking down" botnets.
- Second, private–public partnerships are a two-way street: major private sector companies have a tremendous amount to offer the USG, including insight into network vulnerabilities and adversary activities and technical talent. In particular, the top communication service providers, cloud service providers, and cybersecurity companies have visibility across vast networks and data storage systems



Source: Reproduced from GWU CCHS, *Into the Gray Zone*, under a Creative Commons Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0).

Figure 1. Private Sector Active Cyber Defense in the Gray Zone

as well as (despite so many open positions in cybersecurity) a treasure trove of highly capable cybersecurity personnel. In instances involving highly sensitive intelligence, the sharing of intelligence with key communication service providers, cloud service providers, and cybersecurity companies might allow them to modify their services to help a large number of private sector companies, citizens, and the USG. When the information being shared is highly classified, this option can allow the USG to do the most good while working with only cleared companies.

- Third, in some cases, particularly when facing great power cyber intrusions and attacks, the private sector may be overwhelmed. When adversaries are causing more disruption, disinformation, or theft than acceptable from a national level (or than private sector companies can manage), the USG faces a choice of whether to conduct offensive cyber operations to attempt to prevent or deter further attacks. If the USG will not consider such actions, companies may feel compelled to do so, which is a pathway to serious risks of escalation and inadvertent conflict. It is strongly in US interests to ensure that the use of offensive cyber operations is undertaken only by national governments; cyber vigilantism poses significant near-term and (even greater) long-term risks.

There are a number of efforts underway to promote information sharing and cooperation between federal departments and agencies and between the USG and the private sector. For example, the recently initiated Enhance Shared Situational Awareness program aims to "achieve real-time (machine speed) sharing of a cyber-threat information" across federal cybersecurity centers and to expand over time to share real-time information with owners of US critical infrastructure and with US allies.[65] In addition, formal and informal working

[65] Participating federal cyber centers include the Defense Cyber Crime Center (DC3); Intelligence Community Security Coordination Center (IC-SCC); National Cybersecurity and Communications Integration Center (NCCIC); NCIJTF; NSA/Central Security Service (NSA/CSS) Threat Operations Center

relationships have emerged over time between various departments and agencies, in some cases with private sector involvement. Some examples of such relationships include the various infrastructure sector Information Sharing and Analysis Centers (ISACs)/Organizations and the Enduring Security Framework (ESF). The first ISACs were established under PDD-63 during the Clinton administration. During the Bush and Obama administrations, the ESF came into existence and matured, becoming known publicly in 2012 for "scaring the bejeezus" out of private sector CEOs,[66] and is now under the authorities of the DHS-led Critical Infrastructure Partnership Advisory Council.[67]

A key role of the NCDC would be to identify barriers to effective and timely private–public partnerships and to advocate for the necessary changes to improve the overall cyber defense posture of the United States.

The NCDC would not attempt to replace or "take over" federal government department and agency leadership of existing (or future) private–public partnerships. Instead, it would aim to empower and expand them where useful, to facilitate lessons learned between them, and to suggest additional activities that might be of value.

Ongoing information sharing between the federal government and the private sector is valuable but currently falls well short of creating the "greater than the sum of its parts" whole-of-nation approach needed to address the challenges that the United States faces in cyberspace from China and Russia. There are multiple organizational barriers constraining the ability to share information, to conduct integrated planning, and to coordinate operations within the federal government and between it and the private sector. Some, but not all, of these barriers can be overcome with sufficient time and good will in the context of day-to-day cyber responses below the threshold of armed conflict. However, in a fast-developing crisis or conflict, acting at the "speed of relevance" requires real-time information sharing, planning updates, and operational coordination.

A key role of the NCDC would be to identify barriers to effective and timely private–public partnerships and to advocate for the necessary changes to improve the overall cyber defense posture of the United States.[68] Today's US cyber defense system is not set up for operating at the speed of relevance in crisis or conflict, and as a result, in a great power crisis or conflict, there would almost certainly be avoidable failures to "connect the dots" (or avoidable errors in rushing to judgment and incorrectly connecting dots) and to take action in a timely manner.

Engaging State and Local Governments

The NCDC must have strong connectivity with US states and localities to coordinate state-level cyber efforts, including law enforcement and National Guard support. As seen in other national disaster

(NTOC); and US Cyber Command Joint Operations Center (JOC).

[66] Gjelten, "Cyber Briefings."

[67] CISA, "Critical Infrastructure Partnership Advisory Council."

[68] One step the federal government may consider is whether, under limited circumstances, to empower private sector actors to take tactical actions to reach outside their networks to stop imminent threats. This would require the federal government to develop a program aimed at "establishing and regulating 'certified active defenders,' private-sector entities that will operate in conjunction with, and under the direction and control of, the government to enhance cybersecurity resilience." One such model would have some experienced cybersecurity professionals in the private sector serving as members of the National Guard so that if a specific offensive cyber action was authorized, they could be activated under Title 10 authorities, allowing them to make use of the combined resources, infrastructures, and accesses available to both the private sector company and the US government. See Kramer and Butler, *Cybersecurity: Changing the Model.*

response activities, large cities can be on the front lines and can often provide the earliest warnings that an attack is underway. One component of the NCDC, perhaps led by a senior DHS person with an FBI deputy and connected closely to DHS CISA, would be responsible for bringing state and local governments appropriately into the planning process and engaging them in operational coordination. Such planning and coordination could also be facilitated by creating secure collaboration capabilities between state cyber "expert centers" and the NCDC.

Numerous capabilities already exist at the state level. In addition to a state CISO office, states have cyber capability and expertise in their law enforcement entities, homeland security agencies, information technology offices, public universities, and state National Guard. Recognizing this array of expertise, the National Governors Association has noted that twenty-two states have established government bodies to identify and mitigate cyber threats.[69]

Engaging US Allies and Partners

The engagement of key US allies and partners with the NCDC, at various levels of classification, is essential. Coordinating this effort across domestic, defense, and intelligence agencies would require an NCDC element and would be further advanced by assigning a modest number of foreign liaison officers to the NCDC. Such arrangements would help provide mechanisms for better coordinating planning and operational activities at the unclassified and, where appropriate, classified (with release approval) levels.

At the international level, a first step for an NCDC is to increase the coordinated activities of "like-minded" nations and entities. In addition to government-to-government coordination, one additional idea is the creation of an International Cyber Stability Board, consisting initially of a small number of like-minded countries. The member countries would work together to develop protection and resilience for cross-border critical infrastructure for national defense, support campaign responses to cyber-criminal and terrorist actions, and develop other international approaches to the cyber threats presented by Russia, China, North Korea, and Iran.[70]

A continuous net assessment process for cyberspace can be thought of as an ongoing simulation of strategic interactions in cyberspace between the United States and each competitor/adversary (and other relevant players).

NCDC Supporting Function: Provide a Continuous Net Assessment Process

It would be unrealistic to expect the USG and the private sector to effectively plan or coordinate their actions on a day-to-day basis or in crisis/conflict without a shared common perspective of the current situation and an ability to share a visualization of potential future developments. Providing this perspective, through tailored visualization tools based on a wide range of data sources, would be a key role of the NCDC.

Sustaining a shared common perspective requires creating and maintaining a platform for securely sharing data and analytical insights within the USG and with select private sector partners, at appropriate classification levels. Sharing a visualization of potential future developments requires, additionally, a gaming/simulation platform for conducting (human and machine) simulations and analyses aiming to anticipate the most likely and most dangerous future adversary courses of

[69] Kramer and Butler, *Cybersecurity: Changing the Model.*

[70] Kramer and Butler, *Cybersecurity: Changing the Model.*

actions—including responses to actions that the United States might take.

The DSB proposed a continuous net assessment process for cyber in 2019,[71] and the 2020 Cyberspace Solarium Commission proposed development of a Joint Collaborative Environment (JCE), whose role would be to share and fuse threat information, insights, and other relevant data across the federal government and between the public and private sectors. These two ideas are natural complements of each other. Moving forward with a JCE makes good sense, and its role should be extended to support the NCDC's planning—both deliberate planning and planning during crises—and coordination of operations.[72] The JCE would also support the operations of the private sector, state and local governments, and key US allies in the defense of their digital estates.

A continuous net assessment process for cyberspace can be thought of as an ongoing simulation of strategic interactions in cyberspace between the United States and each competitor/adversary (and other relevant players). This process would be supported by intelligence/counterintelligence assessments and informed by tabletop war gaming, modeling and simulation, and results from cyber range activities. The objective is not only to assess the current situation but to assist intelligence analysts, planners, and decision-makers in anticipating potential future adversary courses of action, alternative US options, and how they may interact with each other and with other key actors' choices.

Such a net assessment process would not provide clear-cut "answers" regarding the present situation, let alone the future. However, it would help highlight areas where additional information and intelligence are most needed. Because adversaries are adapting as they exploit emerging cyber vulnerabilities, this net assessment process could also generate testable hypotheses regarding next adversary moves so that intelligence assets can be directed appropriately, defensive measures can be taken, and offensive measures can be preplanned.[73]

Thus, a continuous net assessment process will not "predict" exactly how an adversary may act or respond to US action, or precisely how a crisis will evolve. However, it could provide much better-informed insights into these questions and thus help inform which options are more likely to work better under which circumstances. A continuous net assessment process would also work to identify new intelligence indicators to give early warning that an attack was being prepared or was underway.

If a continuous net assessment process provided only a modest improvement in understanding adversary perspectives and the implications of alternative courses of action, it would add critical insights (and, over time, muscle memory) to inform US choices, provide strategic advantage to the United States, and help avoid serious errors of omission or commission. Given the tremendous uncertainties involved in dynamic interactions in cyberspace and with actions in other domains, identifying what is unknown or uncertain may be at least as important to decision-makers as making an accurate prediction. Thus, the continuous net assessment process would feed risk assessments of various options to decision-makers so that they are able to better understand the relative advantages

[71] From DoD, *Task Force on Cyber*: "The Director of the Office of Net Assessment in the Office of the Secretary of Defense, in coordination with the Under Secretary of Defense for Policy, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, and the Commander USCYBERCOM, establish a continuous strategic net assessment process to support U.S. campaign planning against strategic competitors, adversaries, and rogue regimes. This process should leverage the Intelligence Community, industry, and allied partner capabilities and incorporate persistent red team assessment activity for measuring our effectiveness in cyberspace."

[72] CSC, *CSC Report*.

[73] Alba, "How Russia's Troll Farm Is Changing Tactics."

of various courses of actions (including taking no action).

In order to support a continuous net assessment process, modeling and simulation activities on cyber ranges will be required. In the rapidly changing world of cyberspace, it will also be critical to leverage artificial intelligence/machine learning to test and refine adversarial behavioral models, to develop and evaluate alternative courses of action, and to assess potential unintended and cascading efforts of action (or inaction).

An NCDC would fill a current gap in USG organization and processes relating to cybersecurity.

Accelerating Technology Insertion

NCDC operations will require state-of-the-art tools and processes for planning, decision support, visualization, simulation, and collaboration that help its mission as well as the efforts of departments and agencies. To counter a changing adversary, US national cyber defense efforts must exploit new technologies—for example, artificial intelligence/machine learning—in an operationally relevant setting. Current cyber capability development is lagging significantly behind the stated need to shape, defend, and deter adversaries through denial of benefit and cost imposition.

What an NCDC Would Not Do

An NCDC would fill a current gap in USG organization and processes relating to cybersecurity by integrating department and agency cybersecurity efforts (including supporting information and intelligence) through planning and operational coordination. In understanding the role and mission of the NCDC, it is also important to note what it would **not** do:

- The NCDC would not set strategic direction for the nation; this would remain the job of the NSC. NCDC planning would be conducted under presidential guidance and reviewed in an NSC process. Any proposals for new operational activities or changes in the rules of engagement would be provided to the NSC staff as well as to responsible department and agency heads.
- The NCDC would not have "command and control" authority over department and agency heads. Nor would it supplant or "take over" department and agency roles any more than the joint planning and operational roles of DoD combatant commands (as established in the 1986 Goldwater-Nichols reform act) eliminated the need for the military services. Indeed, the NCDC's success would depend on departments and agencies continuing to build cyber expertise and increased capacity to fulfill their roles.
- The NCDC would not (1) direct operations (the president or the appropriate department and agency heads would do so); (2) conduct operations (departments and agencies would do so); (3) plan or coordinate cyber operations not related to national cyber defense (e.g., military cyber operations aimed at supporting regional combatant commanders); or (4) plan or oversee cyber defense standards or cyber resilience (although another element in the ONCD might take on this role).
- The NCDC would not lead national efforts to combat the theft of intellectual property, counter disinformation, or address other threats in which cyber is just one (albeit important) element in a broader adversary campaign. The NCDC's planning and coordination efforts would be guided by national strategy and policy on such issues, and the NCDC would plan and coordinate the cyber defense–related lines of effort.

NCDC Organizational Relationships, Structure, and Staffing

This section considers where an NCDC might be placed institutionally, how it may be organized, and to whom it should report as well as related issues such as appropriate staffing, enabling technologies, and possible location.

NCDC in the ONCD

The legislation creating the ONCD specifies a range of responsibilities that would be appropriately executed by the NCDC. Reviewing Table 1, below, it is clearly evident that the enabling legislation for the ONCD provides authorities for each of the four key lines of effort proposed for the NCDC: cyber deterrence and supporting norms; active cyber defense; offensive cyber actions in support of cyber defense; and cyber incident management.

Reviewing Table 1, it is clear that the congressionally mandated ONCD is the appropriate place to locate the NCDC. Appendix B provides a detailed assessment of alternative options, such as placing the NCDC within the NSC or in an existing department or agency.

Organizational Structure of an NCDC

The organizational structure of an NCDC could, and probably should, evolve over time. From the outset, its organization should be based on a few key principles.

- The NCDC director should be a senior civilian with both senior-level USG and private sector experience as well as the confidence of the national cyber director and the deputy national security advisor for cyber and emerging technology.

Table 1. ONCD's Statutory Responsibilities Relevant to NCDC

NCDC-Related Responsibility	Excerpt from Statutory Text Creating the ONCD
Cyber deterrence and supporting norms	"coordination of . . . efforts to understand and deter malicious cyber activity" and "diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace"
Active cyber defense	"developing . . . operational priorities, requirements, and plans, . . . ensuring the exercising of defensive operational plans, processes, and playbooks for incident response; . . . ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and . . . reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private sector entities"
Offensive cyber in support of cyber defense	"support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States"
Cyber incident response	"lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, including . . . ensuring and facilitating coordination among relevant Federal departments and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response"
Coordination of USG engagement with the private sector	"ensuring relevant Federal department and agency consultation with relevant private sector entities in incident response; . . . coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate"

Source: House of Representatives, *William M. (Mac) Thornberry National Defense Authorization Act*, sec. 1752, 1950–1963.

- The NCDC vice director should also be an experienced leader, with complementary expertise and background, and would likely be either active duty, reservist, or a member of the National Guard.
- Deputy directors should, as a group, have experience across all key departments and agencies, including the Departments of Homeland Security, Defense, Justice, State, and Treasury as well as various elements of the Intelligence Community.
- All offices (generally under deputy directors) should be organized not by department/agency but by function, with each having an interagency composition and with each being composed significantly of detailees from key departments and agencies.
- To ensure a continued focus on cyber adversaries, critical planning and coordination activities should take place in "country cells" (China, Russia, etc.), and the staffing for each would be drawn from multiple departments and agencies.
- Because the NCDC would be an extraordinarily lucrative target for cyber espionage and attack, it would need a top-notch CIO and CISO and would need to exemplify as well as enable a diverse set of advanced tools and techniques for active cyber defense.
- Personnel responsible for engaging with partners outside the federal government (including key owners of private sector infrastructure, state and local governments, and key US allies and partners) should work to establish effective partnerships with USG departments and agencies as well as facilitate key partners' involvement in core NCDC functions (e.g., plans and operations, intelligence support).
- Federal cyber centers, such as the FBI's National Cyber Investigative Joint Task Force (NCIJTF) and DHS's CISA Central, would continue their work while supporting planning and coordinated campaigns orchestrated by the NCDC.
- Similarly, the Intelligence Community's Cyber Threat Intelligence Integration Center would see the NCDC as a critically important customer; even as it continued to provide strategic intelligence to the NSC, it would build its capacity to provide operationally relevant and timely intelligence to the NCDC.

Figure 2 shows a potential organizational structure for the NCDC. Of particular note, three to five competitor/adversary-focused subordinate cells should be established, with each cell responsible for campaign planning and coordination for cyber defense below the level of armed conflict as well as for contingency planning for cyber defense in the event of conflict. The two cells focusing on China and Russia would be the most important to stand up immediately. Initially, a third cell might address "others," with subcells on North Korea, Iran, and nonstate actors (terrorists and criminal groups) growing into distinct cells over time. Most members of these cells, aside from their full-time directors, should be dual-hatted as staff in one of the deputy directorates (e.g., plans, operations, intelligence support).

Because the NCDC's key role would be to integrate all USG cyber defense actions, personnel from various departments and agencies would be assigned or detailed to rotational assignments.

In addition, because of the importance of building toward a whole-of-nation approach, much of the staff should comprise individuals with private sector experience and active contacts with private sector cybersecurity professionals. Many, particularly

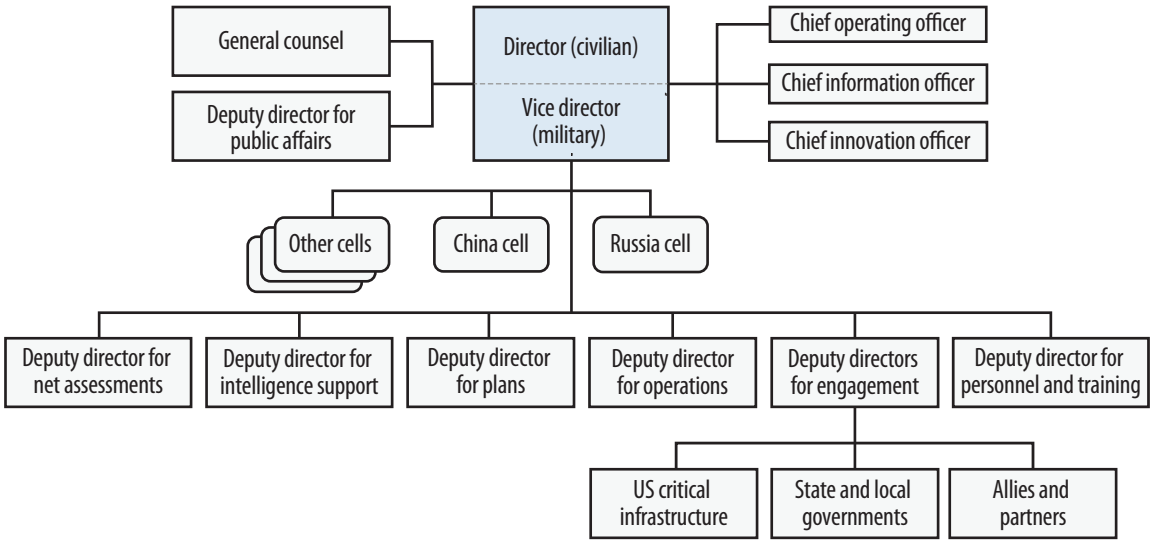


Figure 2. Potential Organizational Structure of NCDC

in the plans and operational coordination deputy directorates, should be National Guard and reserve officers. Personnel from nonfederal government organizations (e.g., state and local governments, private sector companies) should be integrated into staff roles, as security clearances allow.[74]

Leadership and Staffing of an NCDC

The NCDC would be led by a senior civilian and would have a core civilian staff composed mostly of detailees from departments and agencies along with embedded private sector, state and local, and allied liaison personnel.

The national cyber director position is established by statute at level II of the Executive Service, equivalent to the deputy secretaries of major departments. In addition, the national cyber director is to be treated as a principal in the NSC process, equivalent to the chairman of the Joint Chiefs of Staff and the director for national intelligence. This position is clearly senior enough to provide guidance and "top cover" for the NCDC in interagency discussions.

The position of director of the NCDC must be senior enough to allow the recruitment of an experienced, highly regarded individual and so that the person has some bureaucratic "heft" and credibility. This is easily achievable if the NCDC is embedded in the ONCD. The legislation creating an ONCD stipulates that personnel other than the director may serve up to level IV of the Executive Service. This level is sufficient to ensure the ability to recruit a talented senior person to the deputy director position; it is equivalent to Senate-confirmed assistant secretaries of major departments, including the Departments of Homeland Security, Justice, State, Treasury, and Defense. Because the national cyber director is to be considered a principal in the NSC process, if desired, the deputy national cyber director responsible for leading the NCDC could represent the ONCD at deputies meetings relating to cyber defense. This choice would reinforce the "heft" of the NCDC director and also further support the ability to recruit a talented and experienced person to the position.

Because the NCDC's key role would be to integrate all USG cyber defense actions, personnel from various departments and agencies would be assigned or detailed to rotational assignments. Federal cyber interagency activities, such as the

[74] NCDC personnel will need to be cross-cleared into appropriate programs if this organization is going to provide additional value to national security.

FBI's NCIJTF, the DHS's CISA Central, and the Intelligence Community's Cyber Threat Intelligence Integration Center, would continue their work (with modest adjustments) as integral supporting components of the NCDC.

To ensure necessary department/agency expertise in the NCDC and to reinforce key relationships, each department or agency with relevant authorities and operational capacity would have senior personnel detailed on temporary assignments to the NCDC, and these personnel would continue to "wear their institutional hats."[75] For example, military personnel would retain their permanent assignment to US Cyber Command, and the senior military officer at the NCDC would report to the US Cyber Command commander (who in turn reports to the secretary of defense). Similarly, FBI personnel would retain their permanent assignment to the FBI, with the senior FBI agent at the NCDC reporting to the FBI director or their authorized designee (e.g., the director of NCIJTF).

In order to succeed over time, the NCDC will need to compete successfully for at least its share of talented cyber professionals from the USG and (on a rotational basis) the private sector.

It is essential that the NCDC have a talented and well-networked staff, but it could make a significant contribution with a relatively lean staff. The critical planning and coordination activities would take place in each of the "country cells" (China, Russia, etc.); if there were five such cells each with ten people, then fifty people would be needed to fulfill this function. In order to get the needed expertise and connections to key departments and agencies, most of the personnel in the country cells (and many others) would be detailees and assignees from departments and agencies. Under the organization depicted in Figure 2, five of the NCDC deputy directors—for net assessments, intelligence support, plans, operations, and engagement—would have the majority of their personnel embedded in country cells. The deputy director for personnel would need a handful of people to support the recruitment, retention, and morale of personnel. Adding in small offices for the general counsel, chief operating officer, chief information officer, and chief innovation officer as well as public affairs would result in an office at full operating capacity of perhaps one hundred personnel, including the director, vice director, and administrative support staff.

The NCDC could achieve an initial operating capability with fewer than one hundred personnel, perhaps with as few as thirty to forty.[76] It is important to note that although the legislation creating an ONCD caps total personnel at seventy-five, the legislation specifically allows for the ONCD to "utilize, with their consent, the services, personnel, and facilities of other Federal agencies."[77] Thus, with the support of other departments and agencies (if necessary by direction of the president), the NCDC could rely heavily on personnel detailed from departments and agencies. If so, an NCDC of one hundred that was 60 percent detailees would count only against forty of the allowed seventy-five ONCD

[75] The appropriate duration for a temporary detailee (who would retain their department/agency chain of command) would depend in part on the seniority of the position, with individuals in more senior positions generally detailed for a longer duration. On the other hand, individuals who are assigned to the NCDC might be retained for a longer duration if they have unique knowledge (e.g., of Chinese or Russian cyber tradecraft) or skills (e.g., contingency planning or net assessment).

[76] For comparison, the Terrorism Threat Integration Center, precursor to today's National Counterterrorism Center, was initially established in 2003 with "approximately three dozen detailees from across the US Government (USG)." ODNI NCTC, "History."

[77] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395.

slots. Such a model makes good sense in any event: to effectively integrate the authorities of various departments and agencies, the NCDC should in any event be composed mostly of detailees from key departments and agencies.

Because it will be required to integrate domestic and overseas operations and approve many important actions through the NSC process during great power crisis or conflict (when cyber will be one of many issues the NSC must deal with), the NCDC will need to retain close working relationships with a wide range of departments and agencies.

This reality creates an important opportunity for the NCDC to serve as a flywheel for interagency and national-level training and education on cyber defense.

Creating a National Cyber Cadre

In order to succeed over time, the NCDC will need to compete successfully for at least its share of talented cyber professionals from the USG and (on a rotational basis) the private sector. Given the importance of this national center, the president might make a personal appeal to industry CEOs while directing department and agency heads to provide their best to field an all-American cyber defense "dream team." In addition, the NCDC (and ONCD as a whole) should leverage special hiring authorities, including the Intergovernmental Personnel Act, which could allow experts from think tanks, federally funded research and development centers, and university-affiliated research centers to serve in government positions.[78]

Even the most-qualified personnel from departments/agencies and the private sector will require some onboarding and likely some training in the organization and capabilities of other departments and agencies. Moreover, private sector personnel who come to the NCDC on rotation for one to two years would also need to be trained in USG ethics, legal restrictions, organizations, and processes. (These personnel and training requirements are the basis of our proposal in the Leadership and Staffing of an NCDC section that the NCDC organization include a deputy director for personnel.)

Over the course of a decade or so, after there have been five or more rotations of detailed/assigned personnel from the USG and private sector, an informal network within the USG and between the USG and private sector will have been established. If the NCDC averaged seventy personnel over this period with fifty being rotational, there could be a cadre of 250 or more personnel who had rotated through the NCDC.

This reality creates an important opportunity for the NCDC to serve as a flywheel for interagency and national-level training and education on cyber defense (including experiential learning through exercises and real-world operations). An enlightened NCDC leadership would work to maximize this benefit through training and education efforts as well as the encouragement of continued professional relationships among those who had served in the NCDC.

In addition to the necessary technical knowledge, members of an interagency cyber cadre would benefit greatly from having diverse experiences working in various parts of the USG. Today, such mobility is discouraged rather than encouraged, and this must change.

NCDC Relationships with the NSC and DHS

The NCDC's mission would be to develop whole-of-government and whole-of-nation cyber

[78] See https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/.

defense campaign plans and contingency plans and to coordinate their implementation. This mission overlaps with that of both the NSC and the DHS's CISA. It is worth considering how roles and responsibilities would be divided, or shared, among these three entities.

NCDC and the NSC

In the absence of an NCDC, it would make sense for the NSC to organize an interagency working group to conduct cyber defense planning and attempt to coordinate department and agency activities in support of such plans. As noted above, however, the NSC does not have sufficient staffing to adequately fulfill this role and would not be able to sustain its efforts across presidential transitions. With the NCDC in place, the NSC—particularly the deputy national security advisor for cyber and emerging technology—would retain four essential roles relating to cyber defense.

First, of course, the NSC would set strategic direction and provide guidance for planning and coordinating the nation's cyber defense. Such direction and guidance might be signed by the president (as presidential directives or executive orders) and/or could be the output of NSC meetings (including at the Principals Committee, Deputies Committee, or interagency working group level).

The NSC's second key cyber defense–related role would be overseeing implementation of strategy and presidential directives. This role would include assessing the progress of the ONCD (including the NCDC), as well as of departments and agencies, in improving US cyber defenses. In this role, the national security advisor and deputy national security advisor for cyber and emerging technology could be key allies in ensuing that departments and agencies support the NCDC, effectively implement its campaign plan, and prepare for contingencies.

The third key NSC role would be coordinating the integration of cyber defense efforts with broader national security strategy as well as with regional and functional strategies and guidance. This role would require the deputy national security advisor for cyber and emerging technology and staff to work closely with the other deputy national security advisors and staffs, as well as with department and agency representatives, in order to coordinate cyber defense plans and actions with regional strategies and engagement (e.g., China and Russia on one hand, key allies and partners on the other) and with other functional strategies (e.g., protecting US technological advantages, assuring the security and resilience of critical space assets).

It is clear that the relationship between the national cyber director and the deputy national security advisor for cyber and emerging technology will be of critical importance and that each will depend on the other to succeed.

The fourth key NSC role relating to cyber defense requires a balancing act that involves acting as "honest broker" on the one hand and critical enabler of the ONCD on the other hand. This role will require the NSC staff to adjudicate any interagency disputes over NCDC planning and coordination activities while at the same time ensuring that the NCDC and national cyber director have the necessary support (including facilities, funds, and personnel) and the cooperation of key departments and agencies.

It is clear that the relationship between the national cyber director and the deputy national security advisor for cyber and emerging technology will be of critical importance and that each will depend on the other to succeed. Although the national cyber director would serve as a principal in the NSC process and could therefore take issues directly to the national security advisor or president, if such

"escalation" became the rule rather than a very rare exception, it would result in (at best) a poor relationship between the national cyber director and deputy national security advisor and an inefficient process for planning and coordination. The "strategic" role of the NSC and the "operational" role of the ONCD are highly intertwined, and an ongoing and open discourse between these two key leaders will be essential.

NCDC and CISA

The relationship between the NCDC director (dual-hatted as a deputy national cyber director) and the director of CISA at the DHS is both important and complex.[79] In one sense, the CISA director's mission is broader than that of the NCDC, and indeed broader than that of the ONCD, because CISA is responsible for mitigating physical risks to US critical infrastructure as well as cyber risks. On the other hand, because the NCDC director's mission is to conduct integrated cyber defense planning and coordinate actions across the entire USG and with allies and partners (as well as industry), the NCDC director's mission is broader in terms of the communities and capabilities it must coordinate.

Where the Venn diagram of the NCDC director's and CISA director's missions overlap is in the planning and coordination of cyber defense relating to the US private sector and to state, local, territorial, and tribal (SLTT) governments. This overlap deserves particular attention because Congress, in the same legislation establishing the national cyber director, also established a new Joint Cyber Planning Office (JCPO) within CISA. The JCPO's legislative mandate is

> to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests.[80]

Clearly, the JCPO's mandated mission overlaps with the national cyber director's responsibilities as summarized in Table 1, particularly the national cyber director's responsibility for "developing . . . operational priorities, requirements, and plans, including . . . ensuring the exercising of defensive operational plans, processes, and playbooks for incident response."[81]

Three approaches could be followed to address this overlap in mission between the national cyber director's NCDC and CISA's JCPO. A combination of the three is recommended.

Dual-hat JCPO director as NCDC deputy director. First, the director of CISA's JCPO could be dual-hatted as a deputy director of the NCDC, with responsibility for overseeing private sector and SLTT engagement relating to cyber defense. This approach would be efficient in its use of personnel in that the NCDC would not have to establish a separate group to coordinate private sector and SLTT government engagement. A risk of this approach is that the dual-hatted JCPO director/NCDC deputy director could receive conflicting guidance from the CISA director and

[79] The NCDC director and CISA director positions would be at approximately the same level of seniority. The NCDC director could serve a notch higher in the NSC process; as noted previously, the NCDC director could represent the Office of the National Cyber Director at the deputy level in NSC meetings, and the CISA director would report to the deputy secretary of homeland security. At the same time, the NCDC director position would be at (highest) Executive Level IV (with the national cyber director at Executive Level II), while the CISA director is established at Executive Level III.

[80] House of Representatives, *William M. (Mac) Thornberry National Defense Authorization Act*, sec. 1715.

[81] House of Representatives, *William M. (Mac) Thornberry National Defense Authorization Act*, sec. 1752, 1950–1963.

NCDC director. However, the benefit of efficiency makes this approach attractive notwithstanding this potential friction, particularly initially since the national cyber director (and NCDC) and the JCPO will likely be established in parallel.

NCDC provides guidance, oversight, and support. Second, the NCDC director (to whom the JCPO director would report when wearing the NCDC deputy director hat) could provide guidance to the JCPO to prioritize specific private sector and SLTT engagements (e.g., by sector and by company) in support of the national cyber defense campaign plan and could provide specific expectations regarding the capabilities to be developed. The JCPO would then implement this guidance through plans for private sector/SLTT engagement, and CISA would take the lead in implementing these plans. Under this approach, NCDC staff (outside the JCPO) might well engage with private sector owners of critical infrastructure and SLTT governments on a periodic basis (e.g., quarterly, and as requested) to assess whether cyber defense planning and coordination could be improved and to share information and lessons from outside CISA's experience (e.g., from international engagements led by the State Department).

National cyber director coordinates USG–private sector engagement. Third, there must be acknowledgment that the national cyber director's responsibilities extend beyond the NCDC's role, including "efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security" as well as the pursuit of "awareness and adoption of emerging technology that may enhance . . . the cybersecurity posture of the United States."[82] In meeting these and other responsibilities, the ONCD will need to engage the private sector, along with government research agencies such as DARPA, HSARPA, and IARPA,[83] the national laboratories, federally funded research and development centers/university-affiliated research centers, and academia, on current and emerging technologies and techniques to advance cybersecurity. The ONCD need not—indeed must not—attempt to "control" or supervise all federal engagements with the private sector on cybersecurity. But in order to avoid confusing and confounding key private sector partners, the ONCD will need to coordinate with USG departments and agencies (including DHS and CISA) on engagements with the private sector. This ONCD coordination effort can attempt to address any interagency overlaps or concerns regarding private sector engagement, and unresolved issues can be worked through the NSC process.

It is clear that a key role of the NCDC, consistent with the intent of both the Cyber Solarium Commission and the 2021 NDAA, is the strengthening of CISA's capacity to coordinate cybersecurity planning and readiness across the federal government and between the public and private sectors for significant cyber incidents and malicious cyber campaigns. In this context, the NCDC would set planning and operational coordination priorities for CISA as the agency works to strengthen

[82] House of Representatives, *William M. (Mac) Thornberry National Defense Authorization Act*, sec. 1752, 1950–1963. The following excerpt from legislation gives a sense of the breadth of the national cyber director's mission: The national cyber director is "the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of: (i) information security and data protection; (ii) programs and policies intended to improve the cybersecurity posture of the United States; (iii) efforts to understand and deter malicious cyber activity; (iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security; (v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace; (vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and (vii) such other cybersecurity matters as the President considers appropriate."

[83] Respectively, the Defense Advanced Research Projects Agency, the Homeland Security Advanced Research Projects Agency, and the Intelligence Advanced Research Projects Activity.

operational relationships within much of the USG, with industry, and with state and local governments. If a JCPO is established in CISA (as mandated by Section 2215 of the 2021 NDAA), it would make good sense to dual-hat the head of this office as lead for the NCDC's engagement with the private sector and state/local governments.

Organizational Placement and Physical Location

The NCDC would not fit in the NSC, quite literally, given the legislative staffing cap of two hundred NSC personnel. Even if the cap were increased, the NSC staff should be focused on coordinating and overseeing the implementation of strategy and policy, not conducting ongoing campaign planning and coordinating operations.

Placing the NCDC in DHS's CISA, or in another department or agency, would be a prescription for failure. Developing and coordinating the execution of national campaign and contingency plans for cyber defense—plans that really matter—will require departments and agencies to share sensitive intelligence and operational capabilities; a standing interagency body in the Executive Office of the President is needed to make this work. In addition, there is the question of seniority: an NCDC director reporting to the CISA director would sit two levels below the Deputies Committee, whereas an NCDC director reporting to the (principal-level) NCD would operate at the deputies level. Anyone with experience working in the US interagency process understands how important these differences of organizational placement and seniority of the NCDC director would be in practice.

As noted above, in the same defense authorization bill that created the ONCD, Congress mandated the creation of a JCPO in CISA with the mission of developing plans for cyber defense operations. The obvious solution, as noted above, is for the director of the JCPO to be dual-hatted as the lead for private sector and state/local government engagement in the NCDC.

A more mundane question is: Where would an NCDC reside physically? Even with the best virtual collaboration and planning tools, it will be essential to have a cadre of interagency personnel and private sector liaisons who work under the same roof to plan, coordinate, and build mutual knowledge and trust.

Because senior members of the NCDC would need to meet with key department/agency leaders and attend NSC meetings on a regular basis, the NCDC should be located either in or within short driving distance of Washington, DC. Because the NCDC would be an extremely attractive target for foreign espionage, it should be located in a highly secure facility with the best-in-government physical security and cybersecurity. To establish the NCDC without having to wait for a new building construction, it should be placed in a location that has immediately available secure space and some ability to grow.

Placing the NCDC at Ft. Meade would meet all these criteria and also allow easy face-to-face collaboration with US Cyber Command and the NSA. However, if there are alternative locations in the Washington, DC, area that also meet the above criteria and allow a shorter trip to the White House Situation Room and key departments, they should be considered.

How an NCDC Would Operate

An NCDC would use its inherently interagency staff to conduct planning, coordinate already-approved interagency actions, and raise any concerns regarding department/agency noncompliance with the NSC. These actions would be administratively straightforward.

The NCDC director would request approval for new activities from the department(s) or agency head(s)

with the requisite authorities, simultaneously sending the request to the NSC's deputy national security advisor for cyber and emerging technology for interagency consideration. Many requests for approval, such as a revision of a campaign or contingency plan, would be important but not time urgent and so appropriate for the typical approval process, whereas in a crisis or conflict there may be extremely time-urgent requests for action.

For extremely time-urgent decisions, department and agency heads could approve execution prior to interagency consideration (in this case, an operation could be initiated even as NSC consideration was beginning, and the relevant department and agency heads would be accountable for justifying their choice to proceed). In cases that involved both time urgency and a very good understanding of escalation risks, this decision authority could be delegated further—the objective over time would be to have as many actions as reasonable delegated to departments and agencies, with the NCDC providing coordination. Of course, at any time the president may direct execution, or nonexecution, of a proposed new activity.

The following sections address each of these situations.

Process Flow for Routine NCDC Requests

Figure 3 depicts a situation involving a request for presidential approval of a proposal from the NCDC. The request involves the equities of many departments and agencies but is not extremely time urgent. Examples of such a request could include a request for approval of a cyber campaign or contingency plan; approval of a proposed course of action (with alternative options) to impose costs on an adversary in response to a significant cyber attack; or guidance on how to prioritize the use of limited interagency cyber intelligence and operational capabilities in responding to requests for support from a wide range of private sector companies, states and localities, and international allies and partners. In this non-time-urgent scenario involving multiple department and agency authorities, the principal decision-making process would run through a regular-order NSC process.

Figure 3 shows a simple and direct process (the blue arrows), and one might ask: Why not just have the NCDC director accountable directly to the NSC deputy national security advisor for cyber and emerging technology and vest this deputy national security advisor or the national security advisor with all the requisite authorities to approve or disapprove proposed actions by the NCDC? The answer is threefold.

- First, such an arrangement would violate the military chain of command and, more broadly, the basic principle that department and agency heads must have oversight and accountability for the exercise of their authorities. This is not a question of "bureaucratic turf" but of appropriate oversight of departments and agencies, civilian oversight of the military, unity of command, and good governance.
- Second, the limited office of the NSC deputy national security advisor for cyber and emerging technology could not possibly have the breadth and depth of expertise needed to evaluate all actions proposed by the NCDC (which may involve the authorities of all relevant departments and agencies) nor the implications regarding the resources and opportunity costs that departments/agencies would need to apply to meet such requests. Meanwhile, conditions for ill-informed decisions would be set if relevant experts and (supposedly) accountable senior personnel in departments and agencies were bypassed, including those with expertise and statutory authority and accountability for oversight of planning and operations.

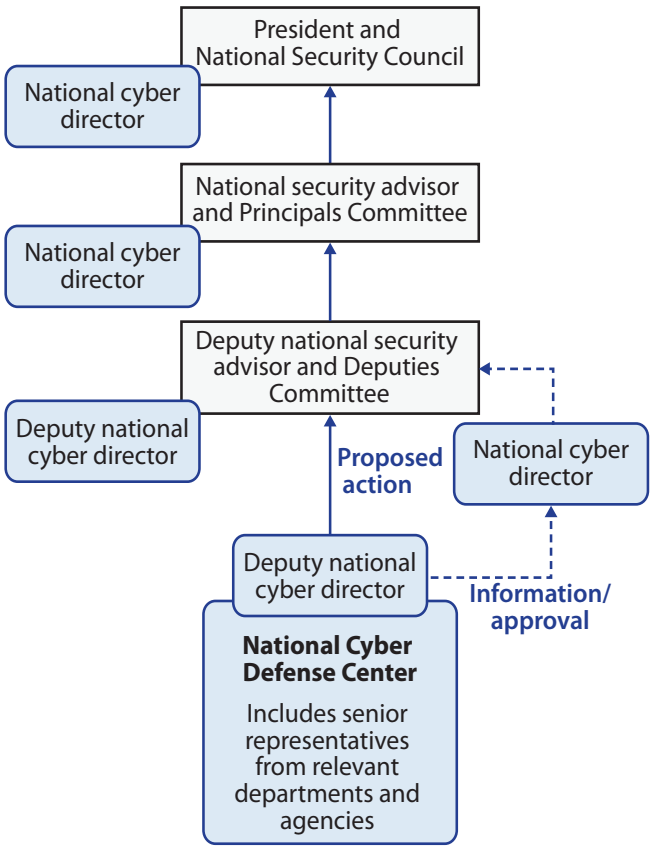


Figure 3. NCDC Proposal Requiring NSC Review and Presidential Approval

- Third, the NSC is, by design, intended to act as an "honest broker" and to perform this role at the strategic level and not the operational level—in other words, it is designed to coordinate strategy, policy, and oversight rather than conduct operational planning or oversight of tactical operations.[84] An operational perspective and a strategic perspective for complex, high-stakes operations are both essential, as is the interaction of these two perspectives in discussion and debate. The NSC staff realistically cannot replicate the expertise of all the departments and agencies; rather, it should require (and question) their inputs.

At the same time, the NSC staff must be very much "in the loop" given the involvement of so many departments and agencies, the novelty associated with cyber operations in a rapidly evolving technology and geopolitical environment, the reality that many operations will be precedent setting, and the high stakes that may be involved. There may be serious strategic risks associated with either doing too little (leading to a weakening of deterrence) or doing too much (leading to diplomatic blowback, retaliation, and potentially unintended escalation) in cyber defense activities. The NSC process is needed, and indeed is designed, to address such issues. On any issue where NSC staff saw a need to conduct an interagency meeting at any level, it would have the authority and the responsibility, as well as the timely information needed, to do so.

At any point in time starting with initial notification, the deputy national security advisor for cyber and emerging technology or the national security advisor could call for an NSC meeting.

Process Flow for Time-Urgent NCDC Proposals

Figure 4 gives an example of the flow of a time-urgent request, in this scenario requiring solely the use of FBI authorities (e.g., domestic law enforcement). Because of the time urgency in this hypothetical example, the director of the FBI may exercise their authorities to approve the request unless the president has directed them not to do so.

[84] The National Security Act of 1947, which created the NSC (and the DoD and Central Intelligence Agency), stipulated that: "The function of the Council shall be to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security." 1947 National Security Act, Pub. L. No. 235, 61 Stat. 496.

Because the hypothetical time-urgent activities proposed by the NCDC in Figure 4 have not been preapproved, requests are made through appropriate FBI channels, even as information flows to the NSC staff and (if assessed to be worth notification) to the president. Of note, the NCDC proposal flows through the FBI's lead for cyber defense, (presumably) the director of the NCIJTF; the NCIJTF would of course have personnel at the NCDC.

At any point in time starting with initial notification, the deputy national security advisor for cyber and emerging technology or the national security advisor could call for an NSC meeting. Moreover, if desired the FBI director or attorney general may decide that there are aspects to the proposal at hand that would benefit from interagency consideration and could request an NSC-hosted interagency meeting—presumably under an established standard operating procedure for time-urgent cyber operations. In the event that the NSC process did not result in consensus in a timely manner, department heads (in this case, the FBI director and the attorney general) could take the matter up directly with the president or, in the case of extreme time urgency, take action under their own authorities, with accountability of course to the president.

It should be noted that Figure 4 is oversimplified in at least three important ways. First, in many or most foreseeable situations, there would be time for expedited NSC decision-making processes to be implemented, and it is important to clearly define and exercise these processes in advance. The model used for the interagency approval of time-urgent counterterrorism operations is a good starting point.

Second, it will be essential to clearly identify who (if anyone) below the levels of the president and department/agency heads has the authority to make specific types of decisions. Developing an expedited decision process and clarifying the

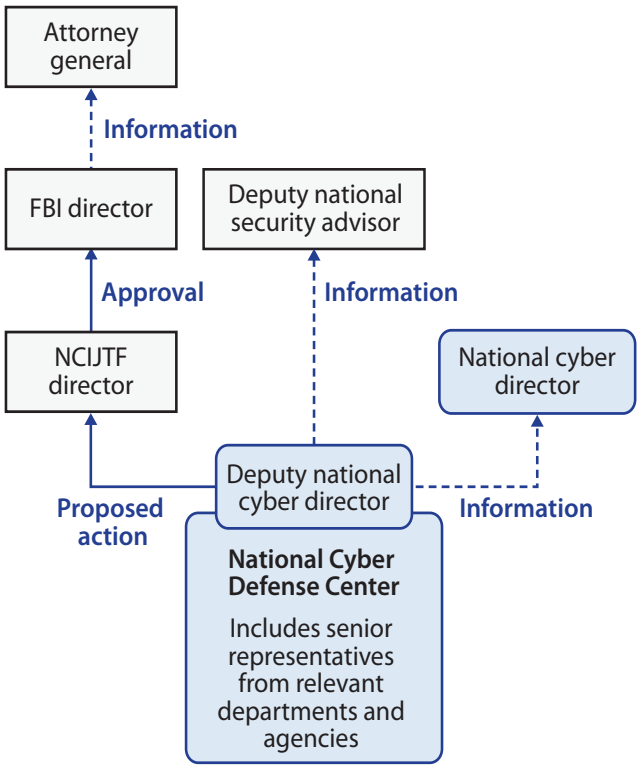


Figure 4. Time-Urgent NCDC Proposal Requiring Approval Only of FBI Director

delegation of authorities for various decisions will be important and require both deliberate planning and tabletop exercises.

And third, in most foreseeable cases, important time-urgent decisions would have implications for agencies and departments in addition to those undertaking action (e.g., prioritization of intelligence collection and analysis based on adversary responses and communication with the private sector). Thus, even in extremely time-urgent cases, there should be a presumption that all parties will share information (but not necessarily have a "vote" on the decision, unless so directed by the president) across all key departments and agencies.

To ensure that the NCDC served as an accelerator and not a brake on sharing information and providing support to the private sector, in many cases departments and agencies would inform the NCDC concurrently as they took actions consistent with planning guidance, including

providing information or support to the private sector. In general, departments and agencies would seek advance approval from the NCDC only in cases where the action being contemplated was contrary to interagency-agreed national priorities or had potential significant costs (e.g., a substantial commitment of resources) or risks (e.g., the loss of sensitive intelligence, diplomatic incident, or escalation to armed conflict).

Setting Conditions for Success

The NCDC's success will depend fundamentally on not only having a well-designed organization and personnel with requisite authorities but also on four other factors. The first priority must be the credibility and competency of the director and other NCDC senior leaders as well as the organization's ability to recruit and train a top-notch core cadre of personnel that is supplemented by knowledgeable and well-networked detailees and assignees from departments and agencies.

Second, and related, is the strong support of the president along with the good faith engagement of key department and agency heads and their senior appointees. This support should be underwritten with a presidential executive order outlining the mission and functions of the NCDC along with the roles for each department/agency in supporting this national security function.

Third, the support of the NSC's deputy national security advisor for cyber and emerging technology and a good working relationship with both the national cyber director and the NCDC director will be essential. Ideally, senior leaders in the NSC should see empowering the national cyber director (including the NCDC) as a key objective.

Fourth, the NCDC will need some budget authority to establish and sustain systems support for continuous net assessment and modeling, which are key to measuring the effectiveness of NCDC planning and coordination activity. Initially, resources could be provided by departments and agencies, but the sooner the NCDC leadership has authority and accountability for building a strong institution and supporting systems, the better. None of these factors can be taken for granted; all must be addressed in the implementation of this proposal.

An NCDC can provide improved day-to-day integration of national efforts across departments and agencies, faster and higher-confidence national decision-making regarding cyber, and thoughtful contingency planning that will reduce risks of inadvertent escalation while bolstering deterrence.

Conclusion

The cyber threat to US national interests is real, and it is growing. Serious shortfalls exist today in the ability of the United States to conduct campaign planning and coordinate cyber defense efforts below the level of armed conflict, and there is a dangerous lack of planning and preparation for national cyber defense in the context of a great power crisis or conflict.

An NCDC would bolster the US strategic position in cyberspace, especially relative to great power competitors China and Russia. It would provide a major step function increase in the USG's ability to integrate the spectrum of interagency authorities and capabilities necessary to cyber defense.

An NCDC would not eliminate the need for departments and agencies to have strong cybersecurity capabilities; rather, it would help give them greater focus and closer coordination. Like all organizations, an NCDC will have growing pains and will make mistakes; the goal should be to advance to

a mature organization within a reasonable period (e.g., two to three years), after making most of its mistakes in war games, simulations, and relatively low-risk cyber intrusions rather than in the context of a great power crisis or conflict.

In order to be successful over the long term, the NCDC will need to help develop a cadre of interagency-trained cyber professionals and to spur the continued development of state-of-the-art tools for collaborative planning, visualization, simulation, and decision support. Although an improved US posture in cyberspace is not guaranteed with an NCDC, it is far more likely.

Put differently, if an NCDC existed today and functioned even reasonably well in its planning, operational coordination, and net assessment functions, any proposal for its elimination would be seen clearly to leave a major gap in the ability of the USG to compete, deter, and if necessary, fight and manage escalation in cyberspace. That cyber defense gap exists today and is evident to US competitors and adversaries, thus putting US national security at avoidable risk.

Appendix A The Evolution of US Cyber Defense Strategy

The US government (USG) strategy for cyber defense has evolved dramatically over the past three decades, and a number of USG organizations have been established to deal with the rapidly evolving challenges in cyberspace—often in response to specific cyber incidents.

Initially focused at the advent of the information age in the 1980s on reducing the vulnerabilities of telecommunications and information technology that directly supported national security departments and agencies, US strategy broadened over time to address the vulnerabilities of government networks and privately owned US critical infrastructure. As serious cyber attacks below the level of armed conflict mounted and it became clear that critical infrastructure vulnerabilities were likely to remain for many years, the United States shifted its strategy to incorporate deterrence and interdiction of threats.[85] By the late 2000s, strategy began to emphasize expanded cooperation with the private sector and allies and also began to impose costs on attackers through diplomatic, economic, and law enforcement actions. By 2017, many observers concluded that this modified strategy was not deterring attacks below the level of armed conflict, and US cyber defense strategy shifted to the more proactive approach of "Defend Forward" exemplified by US Cyber Command's new operating concept of persistent engagement to impose costs and degrade adversary capabilities through active cyber defense actions below the level of armed conflict, such as public disclosure of adversary cyber tools and tradecraft.

US Cyber Strategies and Organizations for the Early Internet

In November 1988, the Morris worm disrupted six thousand of the estimated eighty-eight thousand computers (many USG-owned) then connected to the nascent internet.[86] Although the damage from the Morris worm was limited, the risk of future disruption was recognized. As a result, the Defense Advanced Research Projects Agency, which had sponsored the development of the Arpanet, funded the establishment of the first-ever Computer Emergency Response Team (CERT) at Carnegie Mellon University.[87]

In July 1990, the George H. W. Bush administration issued *National Security Directive 42 (NSD-42): National Policy for the Security of National Security Telecommunications and Information Systems*. Of note, this directive focused relatively narrowly on redressing the vulnerability of national security systems—in other words, "telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information, or . . . involve intelligence activities."[88]

Given the relatively narrow scope of NSD-42, which did not include other USG networks (which were few at the time) or civilian critical infrastructure, the National Security Agency (NSA) director was designated

[85] White House, *National Security Presidential Directive*.

[86] Holohan, "As the Morris Worm Turned."

[87] Now known as the Computer Emergency Response Team Coordination Center (CERT/CC). CERT/CC is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University. Since 2003, SEI has also hosted the separate US-CERT, which, under sponsorship from the Department of Homeland Security, serves as the national computer security incident response team. See https://www.sei.cmu.edu/about/divisions/cert/.

[88] White House, *National Security Directive 42*.

as national manager and made responsible for (among a long list) assessing and certifying the security of national security systems. The secretary of defense was designated executive agent for this effort.

Before the end of the decade, it became clear that the implementation of NSD-42 was inadequate to deal with the vulnerabilities posed by a rapidly growing US reliance on the internet. Efforts had fallen short in two regards.

First, national security systems remained highly vulnerable. In 1997, the Department of Defense (DoD) conducted a classified exercise called Eligible Receiver, in which according to later reports, "utilizing only hacking techniques available publicly, the NSA was able to completely infiltrate the DoD network and gain superuser access into high-priority devices."[89] Less than a year later, in February 1998, the DoD experienced at least eleven attacks on unclassified (but some operationally critical) networks, in an intrusion dubbed Solar Sunrise. The culprits turned out to be three teenagers.[90] Later in 1998, DoD computers were again infiltrated extensively, and in this event, dubbed Moonlight Maze, the culprit appeared to be Russia.[91]

Because of these events and the early strategic focus of US cyber strategy on national security systems, the DoD was the first to create new organizations for cyber. In 1998, the Joint Task Force – Computer Network Defense (JTF-CND) was established to provide "an operational approach to securing its [DoD] information systems."[92] As cyber intrusions continued, DoD organizations evolved. As noted in a detailed history of DoD's evolution on cyber, "at the end of 1999 JTF-CND became Joint Task Force – Computer Network Operations (JTF-CNO) . . . In 2004 . . . the mission of JTF-CNO was rolled into JTF-Global Network Operations (JTF-GNO)."[93] Finally, in 2010, the three key operational cyber elements in DoD (Joint Functional Component Command – Network Warfare [JFCC-NW], JTF-GNO, and the Defense Information Services Agency) were brought together in the newly established US Cyber Command.

Second, there was a growing recognition that civilian-owned critical infrastructures were essential to the operation of the US economy, society, and military—and that these critical infrastructures were substantially and increasingly vulnerable to cyber attack. The 1997 report of the President's Commission on Critical Infrastructure Protection, chaired by Robert T. Marsh, concluded that "our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs associated with an effective attack continue to drop."[94]

Based on a recognition of the growing reliance of both government and privately owned critical infrastructure on vulnerable information technologies, in May 1998, the Clinton administration promulgated Presidential Decision Directive 63 (PPD-63), entitled *Protecting America's Critical Infrastructure*, which highlighted the increasing reliance on cyber infrastructure by public and private enterprises and the pressing need for increased collaboration to improve the security of this infrastructure. The directive

[89] Paape, "Operation Eligible Receiver."

[90] Hildreth, *Cyberwarfare.*

[91] Kaplan, "How the United States Learned to Cyber Sleuth."

[92] USCYBERCOM, "U.S. Cyber Command History." JTF-CND evolved into Joint Center – Computer Network Operations (JTF-CNO) by the end of 1999.

[93] Martelle, *Joint Task Force – Computer Network Defense*.

[94] PCCIP, *Critical Foundations*, x.

established an expanded national-level framework to encourage information sharing and collaboration among various critical infrastructure sectors.

Notably, PDD-63 established the national coordinator for security, infrastructure protection, and counterterrorism, providing a focal point in the National Security Council (NSC) intended to ensure that departments and agencies took the steps necessary to meet PPD-63's far-reaching goals:

> No later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:
>
> - the Federal Government to perform essential national security missions and to ensure the general public health and safety;
> - state and local governments to maintain order and to deliver minimum essential public services;
> - the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services. Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.[95]

Given the extensive vulnerabilities of US critical infrastructure today, it is clear that PDD-63's goals were not met. With the benefit of hindsight, it appears clear that the Clinton administration substantially underestimated the challenges associated with protecting critical infrastructure from highly capable and committed adversaries. The exponential growth of internet usage in the United States, coupled with the increased USG and private sector dependence on commercial off-the-shelf information technology systems and software, vastly increased the attack surface available to adversaries attempting to gain access to US information technology systems. The dominance of a few operating systems and software suites gave attackers far more leverage because they could gain access to multiple systems by exploiting one software vulnerability.

A Growing Cyber Strategy Emphasis on Deterrence and Prevention

Unusually, there was continuity in National Security Council senior leadership on cyber when President George W. Bush succeeded President Clinton in January 2001. Richard Clarke, who had served as national coordinator for security, infrastructure protection, and counterterrorism in the Clinton administration, continued in the same position in the Bush administration and was later named special advisor to the president on cybersecurity.

In February 2003, the George W. Bush administration publicly released its *National Strategy to Secure Cyberspace*, which listed the strategy's first objective as "prevent[ing] cyber attacks against America's critical infrastructures."[96] Although none of this unclassified strategy's five priority action areas included taking proactive action to thwart cyber attacks on the United States,[97] a classified directive (which has not been

[95] White House, *Clinton Administration's Policy.*

[96] White House, *National Strategy to Secure Cyberspace.*

[97] The five priority areas were "I. A National Cyberspace Security Response System; II. A National Cyberspace Security Threat and Vulnerability Reduction Program; III. A National Cyberspace Security Awareness and Training Program; IV. Securing Governments' Cyberspace; and V. National Security and International Cyberspace Security Cooperation."

declassified), National Security Presidential Directive 38, was signed in 2004 by President Bush. In 2005, the Bush administration stood up the JFCC-NW within DoD. JFCC-NW was charged with coordinating DoD's offensive activities in cyberspace.

As noted in one publication, "with wars underway in Iraq and Afghanistan and globally against terrorist networks, the Joint Chiefs . . . issued a standing execute order (EXORD) authorizing action to counter the enemy's use of the Internet."[98] This Countering Adversaries Use of the Internet (CAUI) EXORD and the military campaign that it spawned was the first USG attempt, through organizations like JFCC-NW, to use cyber capabilities to counter the propaganda of al-Qaeda. These cyber attacks proved to be tactically successful but appear to have had little strategic impact; it would take the killing of Osama bin Laden in May 2011 to break the back of al-Qaeda.[99]

Near the end of its tenure, in January 2008, the George W. Bush administration promulgated additional guidance with a new directive on the subject of cybersecurity policy. The scope of this directive, released (with some redactions) under a Freedom of Information Act request, was extremely broad. It is particularly notable that this strategy, which led to the Comprehensive National Cybersecurity Initiative (CNCI), now included a focus on deterrence, prevention, and interdiction:

> Actions taken pursuant to this directive will improve the Nation's security against the full spectrum of cyber threats and, in particular, the capability of the United States to deter, prevent, detect, characterize, attribute, monitor, interdict, and otherwise protect against unauthorized access to National Security Systems, Federal systems, and private-sector critical infrastructure systems.[100]

In addition, the FBI's National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008. The NCIJTF includes personnel from over thirty departments and agencies, and as noted on its website, has "primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation." Moreover:

> The NCIJTF also synchronizes joint efforts that focus on identifying, pursuing, and defeating the actual terrorists, spies, and criminals who seek to exploit our nation's systems. To accomplish this, the task force leverages the collective authorities and capabilities of its members and collaborates with international and private sector partners to bring all available resources to bear against domestic cyber threats and their perpetrators.[101]

Upon taking office, President Obama determined that the CNCI and its associated activities should be integrated into a broader, updated national US cybersecurity initiative that included a heavy emphasis on cyber defense and law enforcement.[102] At the same time, the USG issued its first declaratory policy in cyberspace proclaiming the right to use all means necessary in defending itself from a hostile cyber attack.[103] Soon thereafter, in 2010, the Obama administration took steps to bolster DoD's cyber defenses

[98] Hayden, "Making of America's Cyberweapons."

[99] Hayden, "Making of America's Cyberweapons."

[100] White House, *National Security Presidential Directive*.

[101] FBI, "National Cyber Investigative Joint Task Force."

[102] White House, "Comprehensive National Cybersecurity Initiative."

[103] Chabrow, "White House Unveils Int'l Cybersecurity Strategy."

and consolidate its offensive cyber capabilities by reorganizing the JFCC-NW and JTF-GNO into the newly established US Cyber Command.

The establishment of US Cyber Command was due in part to the awareness that both unclassified and classified networks had been penetrated in 2008 (an attack for which the DoD response was dubbed "Buckshot Yankee") and that more needed to be done to organize a more active cyber defense to thwart these type of threats.[104] Thus, even as the Department of Homeland Security focused on building relationships with the private sector and improving passive cyber defenses such as the perimeter-monitoring Einstein program, in 2010 DoD issued a strategy that identified cyberspace as another war-fighting domain that required active cyber defense measures against increasingly aggressive actions being taken by US adversaries in cyberspace.[105]

In 2013, President Obama signed a top-secret Presidential Policy Directive (PPD) on cyber operations, PPD-20, which aimed to offer a whole-of-government approach to offensive cyber operations in support of cyber defense. An unclassified fact sheet on PPD-20 made clear that the administration would "undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as preferred courses of action."[106] This cautious approach was exemplified in the limited US response to Iranian distributed denial-of-service attacks in 2012 to 2013 that cost the US financial sector tens of millions of dollars. As summarized by an FBI report, the bureau "conducted extensive direct outreach to Internet service providers . . . to provide them information and assistance in removing the malware . . . [so that over time] over 95 percent of the known part of the defendants' botnets . . . [had been] successfully remediated."[107] The FBI-led NCIJTF also conducted Operation Clean Slate during this period to take down an adversary-operated botnet infrastructure.[108] And, after North Korea's 2014 hack of Sony Entertainment, the Obama administration responded principally through law enforcement[109] and engaged diplomatically with Chinese leadership to try to stem the massive Chinese cyber-enabled theft of US intellectual property.[110]

The Obama administration's approach to cyber defense, as of early 2014, was summarized well in a speech by Secretary of Defense Chuck Hagel, who stated that "DoD will maintain an approach of restraint to any cyber operations outside of U.S. government networks. We are urging other nations to do the same."[111] To bolster cyber defenses, the Obama administration took steps soon thereafter to increase sharing of

104 Lynn, "Defending a New Domain."

105 Coleman, "Cyber Intelligence."

106 Obama, *Presidential Policy Directive 20*.

107 In addition, in March 2016, the FBI indicted seven Iranian individuals in federal court. DOJ, "Seven Iranians."

108 Demarest, "Taking Down Botnets."

109 AP, "North Korean Programmer."

110 As noted in the fact sheet released by the White House after a September 2015 meeting between President Obama and President Xi Jinping, "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." White House, "FACT SHEET: President Xi Jinping's State Visit."

111 Alexander, "Hagel, ahead of China Trip."

cyber-related intelligence within the government, establishing the Cyber Threat Intelligence Integration Center in 2015.[112]

The Obama administration took important steps to boost interagency coordination and private–public partnerships on cybersecurity, focusing predominantly on passive cyber defenses and on response to cyber incidents (as opposed to the later Defend Forward strategy's emphasis on active cyber defense and, when necessary, preemptive offensive cyber actions, as discussed below).

PPD-41 on United States Cyber Incident Coordination, signed in July 2016, noted that responding to "significant cyber incidents" in particular required coordination within the USG and established a standing Cyber Response Group within the NSC. It also specified that interagency Cyber Unified Coordination Groups would be formed when needed to "serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate."[113]

Task Force Ares Sets a New Precedent

In May 2016, the Obama administration took a major step toward a more proactive cyber posture, albeit focused on counterterrorism, when the DoD established Task Force Ares "to counter the Islamic State of Iraq and the Levant [ISIL] in cyberspace."[114] From the since-declassified EXORD, it is clear that while DoD was the lead on Task Force Ares, the effort also involved the Intelligence Community and the Department of Justice.[115] The (somewhat redacted) version of the EXORD clearly states the center's mission and makes it clear that it involved more than offensive cyber operations:

> USCYBERCOM will establish a JTF [Joint Task Force] to C2 [command and control] cyber forces IOT [in order to] deny ISIL's use of the cyberspace domain through a multipronged approach . . . IOT prevent attacks against the US and coalition partners, support the broader effort to dismantle ISIL [redacted material] and posture for follow-on [redacted material] CO [cyber operations] . . .[116]

In September 2016, the DoD established a concept of operations for Operation Glowing Symphony, including objectives, measures of effectiveness, and measures of performance.[117] As these precedent-setting cyber operations got underway by the DoD, an interagency process continued. One later press account suggested that "a 30-day assessment of the operation noted that while the joint interagency coordination process is fairly mature, it has not been flexed to synchronize the speed, scope and scale of Operation

[112] ODNI CTIIC, "Who We Are."

[113] White House, *Presidential Policy Directive*.

[114] A declassified version (with redactions) of the classified directive establishing Task Force Ares was released under the Freedom of Information Act. See USCYBERCOM, "USCYBERCOM Fragord 01 to Taskord 16-0063."

[115] The EXORD cites a "trilateral memorandum of agreement among the Department of Defense, Department of Justice, and the Intelligence Community regarding computer network attack and computer network exploitation." See USCYBERCOM, "USCYBERCOM Fragord 01 to Taskord 16-0063."

[116] USCYBERCOM, "USCYBERCOM Fragord 01 to Taskord 16-0063."

[117] This information and excerpts from additional documents released under the Freedom of Information Act can be found at https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

Glowing Symphony. It went on to say that those processes were 'taxed' and matured."[118] Of note, Operation Glowing Symphony also appears to have involved some international partners, including Israel and the Netherlands.[119]

Because the work of Task Force Ares was conducted under the Authorization for the Use of Military Force (passed by Congress in the immediate aftermath of the 9/11 attacks),[120] Operation Glowing Symphony was part of the war against terrorism, building off the limited success of the CAUI campaign led by the DoD. Thus, this effort did not provide a direct precedent for military-led offensive cyber operations in support of cyber defense against state actors, including China, Russia, Iran, and North Korea.

However, Task Force Ares and Operation Glowing Symphony did set precedents for interagency-coordinated DoD-conducted offensive cyber operations aimed at not only responding to but preventing cyber or cyber-enabled attacks[121] while involving key allies and partners. Also of critical importance: the concept of operations was not tied to a physical location but rather the virtual battlefield created by ISIS.[122] A final and important point of continuity was that General Paul Nakasone initially led Task Force Ares and was confirmed as commander of US Cyber Command and director of the NSA in April 2018.

Congress and Others Call for a More Active Strategy of Deterrence and Prevention

When Russia used cyber-enabled information operations to "influence the [2016] election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government," the Obama administration responded with economic sanctions on nine Russian entities: "two Russian intelligence services (the GRU and the FSB); four individual officers of the GRU; and three companies that provided material support to the GRU's cyber operations."[123] To many observers, the administration's response, undertaken in late December 2016, appeared too limited to have any prospect of deterring future Russian cyber attacks and information operations. As noted later by Senate Armed Services Committee ranking member Jack Reed, "In 2016, the Russians essentially had an open playing field."[124]

---

[118] Pomerleau, "What New Documents Say."

[119] The Operation Glowing Symphony notification plan, mostly redacted when released under FOIA, "reveals only that Israel and The Netherlands played some unknown role in Operation GLOWING SYMPHONY which warranted the listing of their respective POCs (points of contact) at the bottom of each page." Martelle, *Joint Task Force ARES*.

[120] Authorization for Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224.

[121] USCYBERCOM, "USCYBERCOM Fragord 01 to Taskord 16-0063."

[122] Email communication between Lieutenant General Tim Haugh, former Task Force Ares commander, and the co-author (Butler), November 2020.

[123] The Obama administration's constrained approach was evident in the conclusion to this fact sheet: "Cyber threats pose one of the most serious economic and national security challenges the United States faces today . . . And as we have demonstrated by these actions today, we intend to continue to employ the full range of authorities and tools, including diplomatic engagement, trade policy tools, and law enforcement mechanisms, to counter the threat posed by malicious cyber actors . . ." See White House, "FACT SHEET: Actions in Response."

[124] Nakashima, "Pentagon Launches First Cyber Operation."

As cyber intrusions and cyber attacks on the United States continued despite law enforcement and diplomatic efforts,[125] it became increasingly clear to many observers that a more assertive approach must be considered. In December 2016, Congress mandated that the administration provide "a report on the military and nonmilitary options available to the United States for deterring and responding to imminent threats in cyberspace and malicious cyber activities carried out against the United States by foreign governments and terrorist organizations."[126] As noted by two former DoD civilians, this congressional requirement was "an attempt to force the Administration into articulating a stronger and clearer public policy to deter cyber attacks."[127]

As adversaries' aggressive and persistent malicious cyber activities continued unabated, a consensus began to emerge that a more assertive US approach below the level of armed conflict was needed. In early 2017, the Defense Science Board released a report on cyber deterrence that noted that "responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation (and quite possibly intelligence loss), but not responding carries near-certainty of suffering otherwise deterrable attacks in the future."[128] A subsequent Defense Science Board study, published in early 2018, was even more direct, concluding that "current cyber strategy is stalled, self-limiting, and focused on tactical outcomes" and that "policy guidance is both essential and currently at odds with effective use of cyber capabilities."[129]

US Strategy Shifts to "Defend Forward"

In April 2018, US Cyber Command put forward a bold vision calling for a new approach that centered around two related concepts (discussed in detail below): persistent engagement and Defend Forward. Then, over a two-month period in mid-2018, just in time for the US midterm elections, five key additional Trump administration documents reinforced this new approach.

When released in April 2018, US Cyber Command's new command vision, *Achieve and Maintain Cyberspace Superiority*, outlined a marked departure from earlier approaches. The new vision called for persistent engagement in order to "Defend Forward." As explained in the command vision statement:

> Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate—globally, as close as possible to adversaries and their operations. It describes when we operate—continuously, shaping the battlespace. It describes why we operate—to create operational advantage for us while denying the same to our adversaries.[130]

[125] Paganini, "Biggest Cyber-Security Incidents of 2016."

[126] National Defense Authorization Act for 2017, Pub. L. No. 114–328, 130 Stat. 2000, Sec. 1654.

[127] Snyder and Sulmeyer, "Decoding the 2017 NDAA's Provisions."

[128] One of the authors (Miller) served as co-chair of this Defense Science Board task force, and the other (Butler) served as a member of the task force. DoD, *Task Force on Cyber Deterrence*.

[129] DoD, *Task Force on Cyber as a Strategic Capability.*

[130] USCYBERCOM, *Achieve and Maintain Cyberspace Superiority*, 6.

On August 13, 2018, Congress passed the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, which provided a critical foundation for strategy and process changes that were then underway in the Trump administration. Section 1632 of the NDAA clarified that "military activities or operations in cyberspace short of hostilities" could be considered traditional military activities and, as a result, could be conducted by DoD under Title 10 military authorities.[131] Importantly, as discussed further below, the 2019 NDAA also established a new Cybersecurity Solarium Commission to "develop a consensus [across the USG] on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."[132]

Just two days later, on August 15, 2018, President Trump signed *National Security Policy Memorandum (NSPM) 13*, an executive order that replaced the Obama administration's PPD-20. According to public reports, including the memoir of then-national security advisor John Bolton, this classified directive called for a more assertive and decentralized approach in which departments and agencies could take actions in cyberspace in defense of US national interests.[133]

On September 18, 2018, DoD published a new *Defense Cyber Strategy*, which reaffirmed the US Cyber Command strategy and foreshadowed a new White House strategy by stating, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[134] The *Defense Cyber Strategy* reiterated the US Cyber Command vision statement's call to Defend Forward through persistent engagement by challenging adversary activities wherever they operate in order to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[135] In implementing this new approach, US military cyber forces were not authorized to operate domestically in "blue space" (US domestic cyberspace), instead focusing efforts on "red space" (adversary cyberspace) and "gray space" (cyberspace outside of the United States and the adversary in question).[136]

On September 20, 2018, the Trump administration published its first *National Cyber Strategy*, which had as one of its key pillars to "deter and, if necessary, punish those who use cyber tools for malicious purposes."[137] This White House strategy was notable for being the first national cyber strategy published in fifteen years, as well as for its content. Then-national security advisor Bolton was explicit in giving public notice that the US approach was changing, stating that "for any nation that's taking cyber activity against the United States, they should expect . . . we will respond offensively as well as defensively," adding that "we're going to do a lot of things offensively."[138]

---

131 John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515. Section 1632 affirms the authority of the secretary of defense to direct "military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace . . ." These clandestine activities or operations will be considered "traditional military activity," as defined in the National Security Act of 1947.

132 John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515.

133 Vavra, "Here's What John Bolton Had to Say." See also Pomerleau, "New Authorities." Note that NSPM-13, published in August 2018, can be used by any department or agency. The document remains classified.

134 DoD, *Summary: Department of Defense Cyber Strategy 2018*, 1.

135 DoD, *Summary: U.S. Department of Defense Cyber Strategy 2018*, 1. See also Borghard, "U.S. Cyber Command's Malware Inoculation."

136 Pomerleau, "Two Years In."

137 White House, *National Cyber Strategy.*

138 Liptak, "John Bolton." See also Nakashima, "White House Authorizes.' "

Defending Forward in the 2018 and 2020 US Elections

The USG has become more assertive in defending its national interests through actions in cyberspace, as exemplified by the reported US Cyber Command disruption of the Russian Internet Research Agency "troll farm" during the 2018 US midterm elections and reported analogous actions before, during, and after the 2020 US presidential elections.[139]

A key example of this new approach to US cyber defense was DoD's stand-up of the Russia Small Group to deal with potential Russian interference in the 2018 midterm election.[140] As US Cyber Commander General Nakasone later noted, "We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts."[141]

In March 2020, General Nakasone offered a remarkably detailed statement in open testimony to Congress, which shed new light on CYBERCOM's actions in 2018 and plans for the 2020 elections:

> Last year, we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond. The group reports directly to me and is led by representatives from Cyber Command and the National Security Agency. Its objectives are to generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere. To be sure, we place a high priority on collecting and sharing information with our partners at DHS and FBI to enable their efforts as part of a whole-of-government approach to election security. But Cyber Command's authorities mean that it must also be prepared to act.
>
> In 2018, these actions helped disrupt plans to undermine our elections. During multiple "hunt forward" missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.
>
> Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.[142]

This new, more assertive approach to cyber defense was instantiated in the Election Security Group and remained in place during (and indeed after) the November 2020 US elections. This DoD-led effort also aided other departments and agencies—for example, by sharing indicators of potential compromise with

[139] Regarding 2018, General Nakasone testified on February 14, 2019, that "we created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts." Lopez, "Cyber Command Expects Lessons." Regarding 2020, see, for example, Barnes, "U.S. Cyber Command Expands Operations." See also Cohen, "US Cyber Command Expands Operations."

[140] See Lopez, "For 2020 Election."

[141] Lopez, "Cyber Command Expects Lessons."

[142] *Hearing on the Fiscal Year 2021 Budget Request*, statement of General Paul M. Nakasone.

DHS so DHS could work with states to harden the security of election infrastructure and sharing threat indicators with the FBI to bolster that organization's efforts to counter foreign trolls on social media platforms.[143] General Nakasone noted on Election Day 2020 that he was "very confident in the actions that have been taken against adversaries over the last several weeks and several months to ensure they are not going to interfere in our elections."[144]

It is important to highlight that the Defend Forward approach also involved increased overseas partnerships. In 2018, US Cyber Command deployed personnel to Montenegro, North Macedonia, and Ukraine in its "hunt forward" effort, partnering with DHS and the FBI to release malware publicly.[145] In 2020, US Cyber Command's efforts expanded to include (at least) Estonia.[146] Based on this cooperative effort and less than a week before the 2020 elections, the press reported that US Cyber Command "uploaded samples of the new ComRAT and Zebrocy versions on its VirusTotal account, while the Cybersecurity and Infrastructure Security Agency, in cooperation with the Federal Bureau of Investigation's CyWatch, published two security advisories describing ComRAT and Zebrocy's inner workings."[147]

Such cooperative efforts, including the public release of malware signatures, is part of a "cost imposition" effort to attempt to deter, or at least reduce the scope of, Russian cyber intrusions and cyber-enabled disinformation efforts. As noted by the Estonian Defense Forces' Cyber Command's Deputy Head Mihkel Tikk: "If we discover the malicious activity and we share it with the world, our partners, then attacking is more expensive. So the adversary has to start making decisions and making choices about who they attack."[148]

Expanding international cooperation not only helps in the day-to-day cyber competition below the level of armed conflict, but also can help bolster partnerships and alliances in ways that support deterrence of armed conflict. Former secretary of defense Mark Esper offered some insight into an important connection between cyber activities below the level of armed conflict and the US posture to deter and if necessary fight through a contested cyber environment:

> Defending forward allows us to disrupt threats at the initial source before they reach our networks and systems. To do this, we must be in a position to continuously compete with the ongoing campaigns being waged against the United States. Not only does this protect us day-to-day, but enacting this strategy builds the readiness of our cyber warriors so they have the tools, skills and experience needed to succeed in conflict.[149]

Summary and Looking Ahead

US cyber defense strategy evolved significantly from the 1980s to present day. The first major shift was in scope, from a focus on national security systems to the much broader set of government and critical

143 *Axios*, "NSA Director Says."

144 Sanger and Barnes, "U.S. Tried a More Aggressive Cyberstrategy." See also Lopez, "Cyber Command Expects Lessons."

145 Vavra, "Cyber Command Deploys Abroad."

146 US Cyber Command, "Hunt Forward Estonia."

147 Cimpanu, "US Cyber Command Exposes."

148 Barnes, "U.S. Cyberforce Was Deployed to Estonia."

149 Garamone, "Esper Describes."

private sector systems that sprang into existence as the internet and connectivity expanded dramatically in the United States and globally. The second major shift was in the approach (or "ways" of the strategy, in the ends-ways-means construct): by late 2016, it was broadly recognized that a passive defense-only approach to the cybersecurity of US elections and other critical infrastructure would fail in the face of the technical skills and scale of Russian and Chinese cyber attackers in particular. In order to defend American national interests, a more assertive and proactive approach was clearly needed.

This new approach, first articulated in early 2018 in US Cyber Command's new vision statement and subsequently reiterated in DoD and national strategy documents, represented a marked shift. Although some questioned whether such an approach would work and others feared it might result in escalation,[150] to date the results of applying this new strategy in the 2018 and 2020 US elections appear extremely promising: substantial foreign interference in US elections appears to have been prevented, with no apparent signs of serious escalation risks. This is an impressive achievement given the time constraints in 2018 (the Russia Small Group effort began in earnest only weeks before the election) and the much larger scope of the Election Security Group's efforts in 2020 (USG efforts had to expand to counter not only Russian but also Chinese and Iranian cyber-enabled information operations).[151]

The apparent success of the Defend Forward strategy in negating threats to the 2018 and 2020 US elections suggests that this approach is likely to be sustained in some form and perhaps expanded in the future to address a broader range of cyber threats; for example, this strategy might be used to protect sensitive information and intellectual property, counter malign disinformation and propaganda campaigns, and deter or prevent cyber attacks against US and allied/partner critical infrastructure. If so, a next natural and sensible evolution would be to move toward a stronger integration of all tools of national power in an integrated whole-of-government effort that attempted to establish more effective cyber deterrence, bolster international norms of appropriate behavior in cyberspace, expand international cooperation, and establish routine processes to better anticipate and negate potential future adversary moves.

[150] Healey, "Implications of Persistent (and Permanent) Engagement."

[151] Barnes, "U.S. Cyber Command Expands Operations." See also Starks, "Russia, China and Iran."

Appendix B Alternative Models for a Whole-of-Nation Approach to Cyber Defense

Since recognizing the strategic importance of cyber vulnerabilities associated with government and privately owned critical infrastructure, the US government has taken useful steps to move toward a whole-of-government and whole-of-nation approach for *responding* to significant cyber incidents. Presidential Policy Directive 41's establishment in 2016 of a National Security Council (NSC) Cyber Response Group as well as interagency Cyber Unified Coordination Groups, which are to be formed in response to specific significant cyber incidents, is an important example. However, since 2018, the United States has increasingly focused on preventing significant cyber incidents, including through the Russia Small Group and Election Security Group. While establishing interagency coordination groups after a cyber incident occurs makes sense for responding to cyber incidents, of course this after-the-fact model does not advance the nation's ability to plan and conduct proactive cyber defense efforts to prevent an incident or attack from occurring in the first place.

Certainly, interagency planning and national coordination are no less important for cyber defense than for cyber incident response. Thus, a different interagency model is needed to support a proactive cyber defense strategy.

In order to pursue a whole-of-government and whole-of-nation cyber defense, it will be essential to establish a standing interagency group responsible for planning and coordinating US government cyber defense actions and engaging the private sector and other partners as appropriate. A standing interagency group focused on active cyber defense would add to, not replace, the cyber incident response model. Incident response will still be needed because the combination of cyber deterrence, active defense, and preemption will sometimes not prevent cyber intrusions and attacks; at the same time, continuing active defense during a cyber incident will be essential.

Moreover, close coordination between incident response and active cyber defense in particular is critical because a key part of incident response should be to engage in (and bolster) active cyber defense. Moreover, incident response and active cyber defense are likely to rely on an overlapping group of cyber experts and involve engaging the same government and private sector organizations that have been the victim of intrusion or attack.

Thus, if the active cyber defense model exemplified by Defend Forward is to be expanded beyond protection of US elections to include all tools of national power, a standing task force (or center) will be needed.

If a standing task force or center is to be established, two initial questions must be addressed:

- First, should multiple task forces or a single task force/center for cyber defense be established? We argue in the below subsection that a single task force or center is the strongly preferred approach.
- Second, if a single task force or center is established, where should it be placed institutionally? As explained in the second subsection below, such a center, which we label the National Cyber Defense Center (NCDC), should be embedded in the newly established Office of the National Cyber Director (ONCD).

Multiple Cyber Defense Task Forces or a Single NCDC?

There are three models for expanding interagency task force planning for cyber defense: (1) multiple functionally focused task forces; (2) multiple adversary-focused task forces; or (3) a single task force or center with subordinate "cells" focused on key problems. We consider each option in turn below.

Model 1: Multiple Functionally Focused Task Forces

Under the first model, the US government would attempt to replicate the success of the Russia Small Group and Election Security Group by establishing separate standing task forces for planning and coordinating cyber defense in each substantive area of concern. Under this approach, in addition to sustaining the Election Security Group's work, a second task force on countering foreign disinformation, a third task force on preventing theft of intellectual property, and multiple additional standing task forces focused on protecting the operations of systemically important critical infrastructure (including, for example, designated key operations of the information technology, communications, energy, financial, defense industrial base, and water/wastewater sectors) might be established.

Growing additional functionally focused cyber defense task forces or centers would build directly on the recent successes of the Russia Small Group and Election Security Group. This approach could also leverage existing department and agency assets, including federal cyber centers. For example, the Department of Defense (DoD) Cyber Crime Center could form the initial nucleus for an expanded effort to defend key elements of the defense industrial base, and the National Cyber Investigative Joint Task Force (NCIJTF) within the Federal Bureau of Investigation (FBI) could similarly form the basis for an expanded effort to prevent cyber crime.

Each of these task forces would require not only cyber experts but also experts on the respective functional and related technical topics (electoral processes and supporting systems, social media, intellectual property, critical defense technologies, etc.), as well as experts on adversaries (i.e., on the national leadership perspectives, foreign policy objectives, vulnerabilities, etc., of China, Russia, Iran, and North Korea). Thus, because each task force would need its own cyber experts and experts on adversaries, these new task forces would compete for expert personnel, who would be spread particularly thin.

Each task force would also create an increased demand signal for intelligence on threats and adversary vulnerabilities. These requests for intelligence support would need to be prioritized through a formal process so as not to overwhelm the capacity of intelligence collectors or the Cyber Threat Intelligence Integration Center.

Once established, these distinct task forces would need to coordinate with each other in order to avoid duplicating or (worse) inadvertently undermining another center's efforts to affect a cyber adversary's perceptions; avoid having multiple centers reaching out to the private sector and US allies and partners with similar (or worse, conflicting) requests; and attempt to present coherent and consistent strategic messaging to adversaries and allies alike. Thus, under this first model, it would be critical to have a leadership team through which each of the task forces coordinated their efforts in order to set priorities, allocate resources (including personnel and intelligence taskings), and deconflict if not integrate efforts across centers.

If a national cyber director is established, as mandated in the National Defense Authorization Act (NDAA) for fiscal year 2021, the national cyber director's office would be the obvious choice to act as coordinator of

task force activities. More specifically, the Cyberspace Solarium Commission proposed establishment of a deputy national cyber director for plans and operations,[152] and it would make eminent sense for functional cyber defense task forces to report to this person, who would need a supporting staff in order to provide effective guidance, coordination, and oversight.

Model 2: Multiple Adversary-Focused Task Forces

Under a second model, separate interagency task forces would be established for each key cyber adversary, including, at a minimum, China, Russia, Iran, North Korea, and terrorist groups. (Presumably the FBI's NCIJTF would continue to focus on the criminal cyber threat.) Relative to the first functionally oriented model, an adversary-focused approach would have the substantial advantage of facilitating the development and execution of a campaign effort for each cyber adversary and so could boost the prospects that cyber deterrence campaign plans could be developed, implemented, and adapted over time. This adversary-focused approach would also posture cyber defense task forces to conduct contingency planning for cyber defense in the context of a serious crisis or war.

This second model would share most of the coordination requirements of a functionally focused approach. Clear guidance and daily coordination would be needed to avoid one task force inadvertently undermining another's efforts, to avoid multiple centers reaching out to the private sector and US allies and partners with similar (or worse, conflicting) requests, and to attempt to present a coherent and consistent strategic message to adversaries and allies. In addition, as with a functionally oriented model, task forces for the various adversaries would compete for cyber talent and intelligence support. They also would compete for experts on each of the functional areas of concern (e.g., election security, countering foreign disinformation, protecting intellectual property, and various sectors of critical infrastructure).

Moreover, it would be important to have coordination between adversary-focused groups to ensure that efforts taken against one adversary did not result in fratricide on efforts being pursued for another adversary and to avoid multiple centers reaching out to the private sector and US allies and partners with similar requests. Thus, as with the functionally focused first model, it would be critical to have a single team to which each of the task forces reported in order to set priorities, allocate resources (including personnel and intelligence taskings), and deconflict and (ideally) integrate efforts across task forces. And, as with the first model, if a national cyber director is established, the national cyber director's office would be the obvious choice to lead coordination of cyber defense efforts.

An additional challenge of a distributed adversary-based approach is that, while there are natural department and agency homes that align with and could therefore host some of the functional focus areas (e.g., the Treasury Department for the financial sector, the Department of Energy for the energy sector), there is not a natural department or agency home for cyber defense task forces focused on China, Russia, North Korea, and Iran. Thus, an adversary-focused model with separate task forces for each adversary would require assigning those task forces to one or more departments and agencies (which would undermine the interagency aspect of the task force); embedding them in the NSC staff (which would grow the NSC beyond reasonable size and put its staff in an inappropriate operational role); or assigning them to a new standing body in the Executive Office of the President.

[152] CSC, *CSC Report*.

Model 3: NCDC (or Standing Task Force)

The case for considering a third model starts by noting that any combination of functional (model 1) and adversary-based (model 2) cyber defense task forces would need a higher-level leadership team to establish priorities; allocate resources; and deconflict cyber actions, strategic communication, and outreach to the private sector, state partners, and international partners. In theory, this leadership role could be played by an interagency working group chaired by the NSC staff; however, given the multitude of daily decisions that would be needed, this option would result in slow decision-making and the growth of a large NSC staff (likely larger than feasible under congressionally imposed limits and certainly larger than desirable); and, perhaps more important, it would cause operational and administrative matters to distract senior NSC, department, and agency personnel from matters of strategy and policy.

If a national cyber director is established, then it would make eminent sense to have a deputy director responsible for coordinating the work of various cyber defense task forces. High-level guidance, approval for any major shifts in priorities or approach, any adjudication of concerns from agencies and departments, and integration with functional and adversary-specific strategies (e.g., strategies for the defense of US elections and the defense of intellectual property as well as strategies for China and Russia) would occur through the NSC process.

In this third model, a single leadership team would be responsible for establishing and sustaining appropriate subordinate task forces; for the purpose of clarity, we henceforth refer to this combined task force as the NCDC and its subordinate elements as "cells." The leader of the NCDC would have the flexibility to allocate personnel to various cells depending on need, prioritize requests for intelligence support, and coordinate US government (USG) efforts to build cyber defense partnerships with the private sector and US allies and partners—all of which would be subject to the guidance and oversight of the NSC process and thus, for major issues, subject to the concurrence of key agency and department heads or (if not in agreement) the president's decision.

This third model would allow for a synchronized stand-up and growth plan for a coordinated national cyber defense effort, the ability to prioritize and reallocate resources according to risk assessments or changes in national priorities, and a personnel management approach that made best use of the available team members. Of critical importance, this third model would also allow an integrated planning effort regarding potential crisis or conflict with other countries (particularly China and Russia) so that escalation risks and deterrence opportunities could be identified and evaluated in context. Moreover, as this overarching standing task force built capacity, it could—under appropriate NSC and department/agency direction—serve to coordinate cyber defense of the nation in the event of such a crisis or conflict.

It is clear from the preceding discussion that the third model, establishing an overarching standing NCDC, would carry significant advantages as a means for expanding US cyber defense efforts to build on the success of the Russia Small Group in 2018 and the Election Security Group in 2020. However, this third model raises a plethora of questions, for example: How would it be organized? To whom would it report? How would it operate from day to day and in crisis/conflict? How could USG leaders be sure that this new center did not smother the ongoing initiatives being undertaken by various departments and agencies? And how would department and agency prerogatives, including respect for the military chain of command, be preserved? These questions and others are addressed in the following sections of the report.

Placement of an NCDC within the US Government

Given its role in leading interagency planning and coordinating interagency actions for cyber defense, it is clear that an NCDC must be accountable in some way to the NSC and, at the same time, accountable to multiple departments and agencies. As has been often noted, having multiple bosses is akin to having no bosses, so a key question remains: to whom, below the president, would the NCDC director be principally accountable? We consider the options below.

Option 1: NCDC as an Element of the Office of the National Cyber Director

The NDAA for fiscal year 2021 created a Senate-confirmed national cyber director. The original legislative proposal, submitted by Cybersolarium Commissioner Rep. James Langevin, also called for a deputy national cyber director for plans and operations who would "lead joint interagency planning for the Federal Government's integrated response to cyberattacks and cyber campaigns of significant consequence, to include . . . coordinating with relevant Federal departments and agencies in the development of, for the approval of the President, joint, integrated operational plans, processes, and playbooks for incident response . . ."[153] Although the final legislation passed by Congress quite sensibly did not include specific provisions directing what deputy directors should be established in the national cyber director's office, a deputy national cyber director for plans and operations would clearly perform the same roles proposed in this report for the NCDC director, so it would make obvious sense to combine these roles.

The legislation creating the ONCD specifies a range of responsibilities that would be appropriately executed by the NCDC:

- **Cyber deterrence and supporting norms:** "coordination of . . . efforts to understand and deter malicious cyber activity" and "diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace"
- **Active cyber defense:** "developing . . . operational priorities, requirements, and plans" including "ensuring the exercising of defensive operational plans, processes, and playbooks for incident response; . . . ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and . . . reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private sector entities, as appropriate"
- **Offensive cyber in support of cyber defense:** providing "support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States"
- **Incident response:** "lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence,[154] including . . . ensuring and facilitating coordination among relevant Federal departments

[153] National Cyber Director Act, H.R. 7331. Of note, under this bill a second deputy director would be responsible for strategy, capabilities, and budget; the entire office of the NCD would be composed of no more than seventy-five people.

[154] White House, *Presidential Policy Directive.* A significant cyber incident is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response"

- **Coordination of USG engagement with the private sector:** "ensuring relevant Federal department and agency consultation with relevant private sector entities in incident response" and "coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate"
- **Additional authorities if determined appropriate:** "such other cybersecurity matters as the President considers appropriate"[155]

Thus, if a national cyber director is established, the deputy national cyber director for plans and operations (or a similarly titled deputy director) should be dual-hatted as the director of the NCDC.

Option 2: Establish NCDC as an Independent Task Force Reporting to NSC's Deputy National Security Advisor for Cyber and Emerging Technology

If a national cyber director is not established, then the most obvious option would have the NCDC director accountable to the NSC's senior leader on cybersecurity. Under the Biden administration, this position will be the deputy national security advisor for cyber and emerging technology. Because the job of the NCDC director would be to lead integrated planning and operational coordination across all elements of the US government, only the national cyber advisor (along with the national security advisor and the president) would be in a position to provide oversight of the entirety of the NCDC director's mission and so to have a comprehensive and balanced perspective on the NCDC director's performance.

Reinforcing the NCDC's connection to the NSC process via the national cyber advisor would have a subtle collateral benefit. In any future period of great power crisis or conflict, given the stakes involved and the requirement to coordinate domestic and international actions, some proposed courses of action will likely need to be cleared by the NSC process at an appropriate level. During contingency planning, precedent-setting actions or proposed delegations of authority might be reviewed through a "regular order" interagency process, starting with an interagency working group, with decisions taken by deputies, or elevated to principals and the full NSC or president if needed. In the event of crisis or conflict, time-sensitive operations might follow the NSC counterterrorism model, with a standard format for decision packages supporting rapid decision-making at the deputies level while allowing for escalation to principals and the president when appropriate. The well-practiced lines of communication and trust relationships that would grow out of an NCDC director's accountability would be valuable assets in such situations.

Option 2 has two main advantages. First, it could be accomplished quickly by the administration, and relative to option 1 with a national cyber director, it would not have to await Senate confirmation of an individual to get started. Second, option 2 would allow the NCDC a special status as a White House activity, which could facilitate getting its personnel "read into" sensitive intelligence, capabilities, and programs.

There are two strong, and indeed compelling, counterarguments against option 2. First, there is a long-standing presumption that NSC staff should not be responsible for conducting or directly overseeing

[155] House of Representatives, *William M. (Mac) Thornberry National Defense Authorization Act*, 1950–1963.

operational planning and coordination. Moreover, experience has demonstrated that placing the NSC in an operational role is generally ineffective and sometime dangerous. In addition to the risks associated with this approach (as demonstrated most vividly during the Iran-contra affair of 1985–1987), an operational planning role within the NSC structure would be difficult to sustain over time given the demands on NSC staff for strategic-level guidance and oversight.

Second, under this approach, it is likely that NCDC staff would be "counted" under the congressionally mandated ceiling of no more than two hundred staff working for the NSC. Despite the importance of cyber as a national security challenge, no sensible administration would devote 25 percent, let alone 50 percent, of its NSC staff to cyber defense.

Option 3: Have the NCDC Be Accountable to a Department or Agency

In order to allow the NSC and its staff to focus on strategic issues, the US government has previously placed interagency operational planning and coordination bodies outside of the NSC, under a department or agency. The many federal cyber centers in existence today follow this model, as do the National Counterterrorism Center (NCTC) and National Counterproliferation Center, which both report to the director of national intelligence. As a result of these choices, the scope of these centers' impact is limited and centered around the authorities of their parent organizations. For example, although the NCTC has responsibility for both intelligence integration and national strategic-operational planning for counterterrorism, its principal contribution is on the intelligence side; Central Intelligence Agency and DoD counterterrorism operations are conducted under the guidance and oversight of the president and NSC, not the NCTC.

There is a partial exception to this rule: Joint Interagency Center Task Force South (JIATF South). JIATF South is subordinate in the chain of command to DoD's US Southern Command but its day-to-day operations employ Coast Guard, Drug Enforcement Agency, and other law enforcement authorities, with critical support from the Intelligence Community and State Department, and leverage DoD training missions and (relatively limited) additional resources. In JIATF South's unique organizational model, the JIATF South director is a Coast Guard (rather than Navy) rear admiral—in other words, the leader of the subordinate task force organization is from a different department than the parent organization. JIATF South is perhaps of even more interest given that its operating forces often make use of multiple authorities; for example, they may hand control of interdiction and boarding operations on a naval vessel (the military having authority to detect drug smuggling but not to interdict it) over to Coast Guard or Drug Enforcement Agency officers (who have interdiction authorities) when the time comes to board a ship suspected of carrying contraband.

The NCTC and JIATF South examples suggest that, given the potential downsides and risks of having an NCDC act as an independent agency with accountability principally to the national cybersecurity advisor, if a national cyber director were not established (or were later disestablished), it is worth considering placing the NCDC within a department or agency. There are at least four obvious choices: the Department of Homeland Security (DHS; which, given its responsibility for partnering with the private sector, offers perhaps the most obvious choice); the Intelligence Community (applying the NCTC analogy, this option might promote improved intelligence sharing while limiting the NCTC's role in planning and operational oversight); the FBI (which has already established an interagency NCIJTF); and the DoD (applying the JIATF South analogy, this option might provide valuable enabling resources and effective interagency

coordination in the "field" while allowing leadership of the center to come from another department). We evaluate each of these four options below.

NCDC in the Cybersecurity and Infrastructure Security Agency (CISA). One option would place the NCDC within the DHS, specifically within CISA. This option would build on CISA's role in leading federal government engagement on cybersecurity with the private sector and boost CISA's capabilities and prestige.

There are three serious problems with placing an NCDC in CISA. First, neither CISA nor the broader DHS has the requisite authorities or cadre of experienced personnel relating to three key sets of capabilities central to an NCDC: domestic law enforcement for cyber, foreign intelligence collection, and offensive cyber authorities needed to take action (as opposed to facilitating information sharing) for cybersecurity operations. To reduce this deficit, a CISA director could be hired who had experience working both in the private sector (a central CISA role) and in law enforcement, intelligence, or military cyber operations. In addition, despite the breadth of DHS's mission set, it would be critical that the secretary (or a strong deputy secretary) also be experienced in cybersecurity operations to be able to provide effective oversight and adequately represent the NCDC and CISA in senior-level NSC meetings. Under this approach, a lengthy period of institutional capacity-building would be required, with uncertain results.

Second, and related, if the NCDC were placed within CISA, although it might in theory help enable the CISA director to build internal capabilities, in practice it might just as likely distract the director from this important work. Despite efforts in recent years by a highly regarded, experienced, and energetic director (Christopher Krebs), CISA is a relatively small organization that lacks an operational culture and associated professional cadre. CISA has significantly fewer personnel than either US Cyber Command or the Cybersecurity Directorate within the National Security Agency (NSA) and accounts for only 2 percent of DHS's annual budget, dwarfed by DHS's operational agencies, including the Transportation Security Administration (11 percent), US Immigration and Customs Enforcement (14 percent), US Coast Guard (16 percent), Federal Emergency Management Agency (19 percent), and US Customs and Border Protection (24 percent).[156] Unlike many of its sister agencies in DHS and counterparts across federal cybersecurity, CISA does not have a pipeline of internally developed professionals with an organizational culture focused on achieving measurable success in field operations.

Third, if the NCDC were embedded within CISA, its director would operate three levels below the Principals Committee on the NSC (below the DHS secretary, deputy secretary, and CISA director). This level of seniority, subordinate to three layers of DHS officials, would place the NCDC director at the fourth level of the NSC process, sub-interagency working groups, reducing the ability to recruit a highly capable NCDC director and (relatedly) denying that person the authority and "clout" needed to recruit and retain senior personnel to do the job.

NCDC in the Intelligence Community. If the NCDC were placed as an independent center within the Intelligence Community, its situation would be somewhat analogous to the NCTC and the National Counterproliferation Center. This option could make sense if the most important role of the NCDC were to integrate sensitive intelligence and share it within the federal government, with the private sector (and state and local governments), and with key allies and partners. In this case, the NCDC would function as an expanded version of the National Cybersecurity and Communications Integration Center. An NCDC

[156] DHS, *FY 2021 Budget in Brief*, 7.

placed in the Intelligence Community could also take on a strategic-operational planning function, as the NCTC has done, but (like the NCTC) should not be expected to have a significant impact on departments' and agencies' operations given the limitations of leading high-stakes operational planning from within the Intelligence Community.

The NCTC is an especially useful point of comparison for the NCDC. There are some important similarities between counterterrorism and cybersecurity, including the value of deliberate planning, high stakes that often result in issues being adjudicated in the NSC, and the requirement in some scenarios for quick decision-making. However, cybersecurity operations have three attributes that distinguish them from counterterrorism operations:

- The adversary can perform cyber infiltration of critical infrastructure on US soil at relatively low cost and risk, requiring a sustained campaign with coordinated US governmental actions using a wide range of authorities and capabilities domestically and overseas.
- The US private sector plays a central role, both as a target (especially systemically important critical infrastructure) and as an essential contributor to preventing and responding to attacks.
- Avoiding great power conflict with China or Russia will often be a central concern, so there will be a constant balancing between doing too little (and allowing continued cyber aggression with limited costs) and doing too much (and causing unnecessary escalation while expending impactful cyber attack capabilities that could better serve as a deterrent).

These differences suggest a need for thoughtful advance planning and close interagency coordination for cybersecurity operations as well as a need for effective integration of cyberspace operations into the broader context of political-military objectives relative to China and Russia. Based on experience with the NCTC's strategic-operational planning function, which could be described as having a "light touch" (very limited impact) on the operational planning and actions of the CIA and DoD, such planning conducted from within the Intelligence Community would seem likely to fall well short of the type of detailed operational planning and coordination in cyberspace that is proposed for the NCDC, and needed by the nation.

A critical additional factor is the respective roles of the Intelligence Community and the DHS in the United States. The issue at hand can be understood by considering the United Kingdom's National Cyber Security Centre (NCSC). The NCSC is organized as part of the Government Communications Headquarters (a counterpart to the US NSA), has generally been viewed as successful since its establishment in November 2015, and so might be seen as providing a model for placing the NCDC in the Intelligence Community. However, the NCSC's mission is roughly equivalent in the US system to a combination of DHS's CISA and NSA's Cyber Directorate.[157] Although it is very valuable for these two US organizations to work well together in the United States, there is no rationale (nor likely any political appetite) for moving functions currently in CISA, including the US Computer Emergency Readiness Team, to the Intelligence Community.

Simply put, the NCSC works in the British system of government but is not an appropriate model for the United States. Placing the NCDC in the Intelligence Community—creating essentially a somewhat-expanded Cyber Threat Intelligence Integration Center—could in principle add value by improving information and intelligence sharing within government and between the government and private sector,

[157] Hannigan, *Organising a Government for Cyber*, 18.

but this option would make sense only if it were decided to eliminate (or vastly reduce) DHS's current role in leading private sector engagement. Thus, barring a clear failure of DHS's cyber efforts, this option does not appear feasible or desirable.

NCDC in the Department of Justice. Placing the NCDC in the Department of Justice, likely with the FBI, would carry two main advantages. First, it would allow the NCDC to be built out from an existing interagency group, the NCIJTF. Second, unlike placement in DHS or the Intelligence Community (or the DoD, considered next), this option would place the NCDC in an institutional home that has authorities to gather domestic intelligence and undertake law enforcement actions, as well as a growing record of working with the private sector on cyber (particularly cyber crime).[158]

At the same time, placing the NCDC in the FBI (or elsewhere in the Department of Justice) would bring at least three serious challenges. First, by turning the FBI into the de facto lead for coordinating with the US private sector, it would effectively take over DHS's current role in leading private sector engagement. As with the Intelligence Community option, barring a clear failure of DHS's cyber efforts, undermining DHS's efforts to establish an effective role in cyber defense does not appear politically feasible or desirable.

Second, making the FBI the lead for cyber defense, including proposals for supporting offensive cyber actions, would force the FBI director to be responsible for activities well outside their authorities and expertise. This would both dilute the time available for leadership of efforts in other areas (e.g., domestic counterterrorism) and require extensive coordination with the DoD (particularly US Cyber Command and the NSA). It is important for the FBI director to avoid overstepping by essentially inserting himself into the military chain of command as well as to avoid appearing to have responsibility but simply deferring to the secretary of defense—either would undermine effective senior-level oversight and accountability in this critical arena of national cyber defense.

Third, although since 9/11 the FBI has substantially shifted its mindset to preventing international terrorism rather than focusing only on law enforcement after an attack, it has not made a similar shift to date toward prevention in the cyber defense arena. Nor does the FBI have a deep bench to support cyber incident response. Thus, placing the NCDC in the FBI would amount to betting on a major reorientation of FBI organizational culture and training—a long-term and uncertain proposition. And if the FBI did begin to make this reorientation, there would be concerns in many quarters (likely including from within the FBI) that it could overreach and infringe on the privacy and civil liberties of Americans.

Overall, placing the NCDC in the FBI would appear to carry both more potential benefits and more potential challenges than placing it in DHS or the Intelligence Community. However, given the likely perceived threat to privacy and civil liberties in particular, it does not appear either politically feasible or desirable to place the NCDC in the FBI in the event that an ONCD were not established.

NCDC in the DoD. Placing the NCDC in the DoD would allow it to immediately leverage the two most capable national cyber organizations, the NSA and US Cyber Command. Moreover, the US armed forces have a strong culture and decades of experience in integrated joint (interservice) and combined (international) operational planning and coordination. In addition, there is a somewhat analogous model that has worked well: JIATF South, which conducts counter-narcotics operations and has been described

[158] For more information on FBI intelligence authorities, see https://www.fbi.gov/about/leadership-and-structure/intelligence-branch.

as the "gold standard of interagency operations,"[159] is an element of US Southern Command, a part of DoD. Creative leadership and staffing arrangements have helped JIATF South to function as an interagency body; for example, JIATF South is headed by a Coast Guard admiral and includes representatives from multiple departments and agencies, as well as from many countries.

However, there is a compelling counterargument to having the NCDC within DoD: This choice would make the secretary of defense, and American armed forces, directly responsible for cyber-related law enforcement. The Posse Comitatus Act and other US law "generally prohibit US military personnel from direct participation in law enforcement activities."[160]

Of course, US law could be changed to expand DoD's role. However, there is good reason for such restrictions on the role of US armed forces in US domestic affairs, including protecting the civil liberties and privacy of American citizens as well as minimizing the risks to democratic institutions that would be inherent in having the military take the lead for domestic operations. The US government's cybersecurity capabilities have been organized according to the understanding that DoD will not lead domestic operations, and there would (quite sensibly) be strong opposition in Congress and among the American people to such a militarization of cybersecurity in the United States.

In addition, an NCDC embedded in US Cyber Command would not be able to effectively integrate domestic intelligence or support to key domestic owners of critical infrastructure without a wholesale revision to today's arrangements where DoD is required to avoid collecting domestic intelligence and the DHS is intended to lead engagement with the private sector. The JIATF South model would not work well because for cyber defense, there will be few occasions in which the ability to pass authority from one agency to another in real time is feasible or adequate. Unless and until placement of the NCDC in the ONCD collapses, placing the NCDC in the DoD should be a nonstarter.

Discussion. The fundamental challenge with making the NCDC accountable to a department or agency head is that the proposed scope of NCDC planning and operational coordination encompasses such a broad swath of authorities that no one department or agency is a natural home. Placing the NCDC within any one organization—whether DHS, the Intelligence Community, the FBI, or DoD—would put responsibility for NCDC planning and coordination spanning domestic law enforcement, Intelligence Community, and military cybersecurity operations on the senior officials of a single department or agency that has only a fraction of the relevant authorities. Given this reality, placing an NCDC within an existing department or agency would be clearly inferior to placing it within the ONCD.

Relationship of the NCDC to the NSC Staff

Assuming that the NCDC is placed within the new ONCD—in other words, option 1 above is selected—a follow-on question remains: What should be the relationship between the NCDC and national cyber director on the one hand and the NSC staff on the other? We consider below three alternatives for implementing option 1.

[159] Carter, "Improving Joint Interagency Coordination."

[160] US Northern Command, "Posse Comitatus Act."

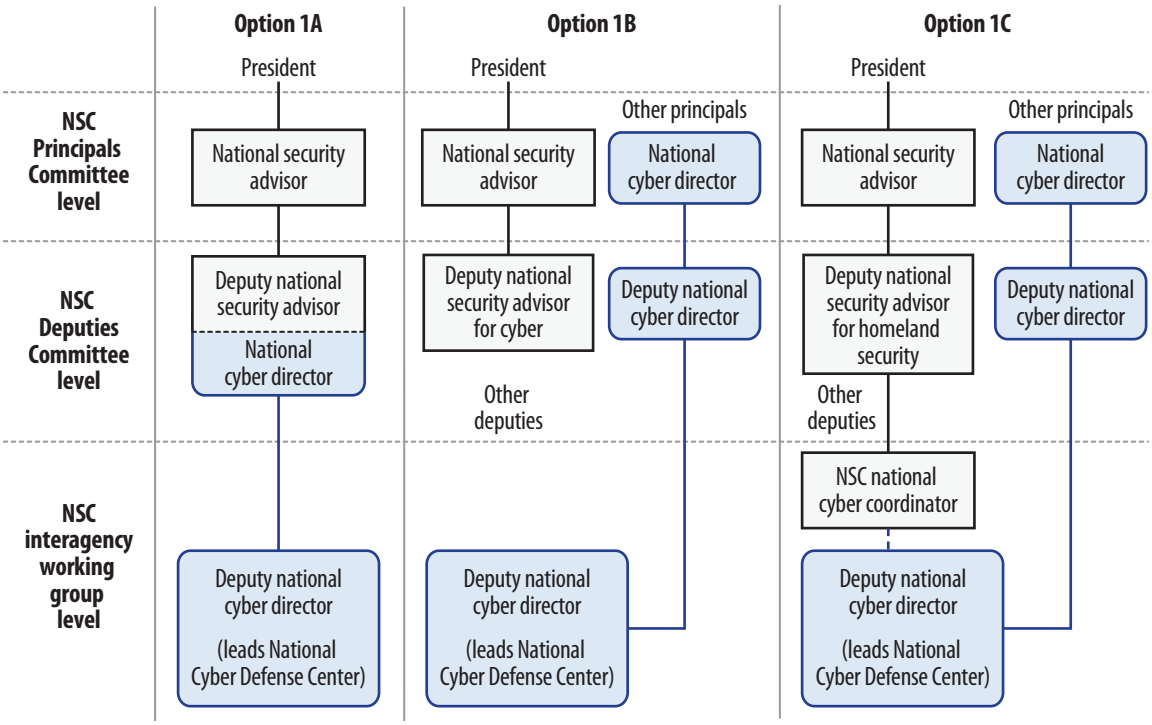


Figure B-1. Organizational Relationships between NCDC and NSC

Option 1A: Dual-Hatted National Cyber Director as Deputy National Security Advisor

In option 1A, the national cyber director is dual-hatted as the president's national cyber advisor and, in addition, is a member of the NSC staff as a deputy national security advisor. Wearing the deputy national security advisor hat, the national cyber director would be responsible for planning and chairing cyber-related meetings of department and agency deputies, establishing an organization and agenda for the subordinate interagency working groups, and teeing up Principals Committee and full NSC meetings. This individual would have a seat at the table for these Principals Committee and NSC meetings but, as an NSC staffer, would not be a principal.

The main advantage of option 1A is that it could create an extremely strong national cyber director. The person in this position would have close proximity to the president on a daily basis, a key role as convener of deputies-level interagency meetings, and a Senate-confirmed principal who is essentially the head of a small agency or center (such as the NCTC).

This approach has three main disadvantages. First, the national cyber director would essentially be "grading one's own homework" because the NCDC staff (i.e., the deputy national cyber director for plans and operations) would be bringing proposals to the interagency process that were already approved by the national cyber director. This arrangement could provoke bureaucratic resistance and encourage department and agency heads to align themselves outside the formal interagency process in advance of NSC meetings; it would also take the NSC staff out of the role of honest broker for cyber-related issues.

Second, given that the national cyber director is to be Senate confirmed, the record-keeping requirements associated with the two distinct "hats" would conflict, and the national cyber director could be put in

the position of being called to testify to Congress regarding private discussions with the president. This situation might be managed, but it would complicate the establishment and efficiency of the ONCD.

Third, Congress has imposed a limit on the total size of the NSC staff, capping it at no more than two hundred professional staff.[161] Given the scale and breadth of the challenges facing the United States, it is simply not reasonable to allocate even thirty (let alone one hundred, or half) of these positions to an NCDC.

On the whole, option 1A is extremely problematic.

Option 1B: National Cyber Director Is a Principal and the NSC Also Has a Dedicated Deputy National Security Advisor for Cyber

In option 1B, the NSC's senior national cyber coordinator is a deputy national security advisor. Under this option, the national cyber director would need to work with the national security advisor or the NSC's deputy national security advisor to establish an agenda for interagency meetings. The Senate-confirmed national cyber director would not chair cyber-related principals or deputies meetings but would attend cyber-related principals and full NSC meetings as a co-equal to other principals, including the director of national intelligence and the chair of the Joint Chiefs of Staff.

If an administration wants to "elevate" cyber as a key issue, option 1B is the preferred choice. Compared with the Trump administration, there would be two new cyber-focused senior interagency positions: the principal-level national cyber director and the deputy national security advisor for cyber. Compared with other recent administrations, the national cyber director position would be new, and the senior NSC person focused on cyber would be elevated one level. In addition to elevating cyber as an issue, this approach would have the advantage of retaining an honest broker role for NSC staff. If the national cyber director and deputy national security advisor for cyber worked closely together, they would form a powerful team.

The main disadvantage of option 1B would be that the deputy national security advisor for cyber would have a "smaller" job than may seem appropriate given the extensive roles of the national cyber director; this could make it more difficult to recruit and retain a top-notch person and could work to reduce their influence over time. However, this downside could be mitigated by dual-hatting the deputy national security advisor for cyber as a deputy economic council advisor or as the NSC lead for cyber and emerging technology. The latter approach makes particularly good sense given how important key technology areas such as 5G, artificial intelligence/machine learning, and quantum computing are to cyber defense and cybersecurity. Either approach could help in attracting and retaining top talent; the latter tech-focused approach has the added advantage of highlighting the criticality of emerging technologies to national and international security.[162]

[161] Sec. 1085 of the NDAA for 2017 specifies that the NSC staff "shall not exceed 200 persons, including persons employed by, assigned to, detailed to, under contract to serve on, or otherwise serving or affiliated with the staff. The limitation in this paragraph does not apply to personnel serving substantially in support or administrative positions." National Defense Authorization Act for 2017, Pub. L. No. 114–328, 130 Stat. 2000.

[162] In early January 2021, Biden indicated that he intended to pursue this latter option, with a new deputy national security advisor for cyber and emerging technology. Bertrand, "Biden Taps Intelligence Veteran."

Option 1C: National Cyber Director Is a Principal and the NSC has a National Cyber Coordinator

Option 1C would bring the NSC senior position for cyber back to its historical level as cyber coordinator, a level below deputy national security advisor.[163] In this model, the NSC cyber coordinator could lead meetings at the interagency working group level (in this option, the national cyber director's staff would likely chair few if any interagency working groups), but the deputy national security advisor responsible for homeland security would chair deputies-level meetings.

Under this option, the national cyber director, as a principal, would be clearly senior to the most senior NSC staffer with full-time responsibility for cyber and would be a peer to the national security advisor. It would be important for the national cyber director and senior staff to establish good working relationships with the NSC cyber coordinator and the deputy national security advisor responsible for homeland security.

The main advantages of option 1C are that it (like option 1B) keeps the NSC staff in an honest broker role and that it (unlike option 1B) forces the deputy national security advisor for homeland security to integrate cyber-related issues into the broader homeland security agenda. This second advantage is also this option's main disadvantage: the deputy national security advisor responsible for homeland security must deal with a wide range of hot-button issues, including counterterrorism, pandemic response, and immigration, and there is a high likelihood that cyber defense (and cybersecurity in general) would be squeezed out. The NSC cyber coordinator just would not have the prestige and rank to drive the cyber agenda to the same degree as in options 1A and 1B.

Discussion

Figure B-1 summarizes the three options considered above.

Option 1A would place the NSC in an operational role, remove the "honest broker" role of the deputy national security advisor for cyber because they would also be dual-hatted as national cyber director, and require congressional approval for a much larger NSC staff. This option should not be considered.

Option 1C would be a clear improvement over the situation during past administrations, with the national cyber director position added and a national cyber coordinator position on the NSC reestablished. The biggest downside to this option is that cyber issues are very likely to be pushed onto a back burner by a deputy national security advisor dealing with COVID-19, counterterrorism, immigration, and a host of other issues. In addition, the national cyber coordinator would not have the same bureaucratic "heft" as a deputy national security advisor and so would be less able to provide support and "top cover" for the national cyber director.

Thus, option 1B, which would add two new strong positions to the national effort on cyber, would be strongly preferred. If this option is pursued, it will be critical that the national cyber director and the deputy national security advisor for cyber and emerging technology work well together and indeed that the deputy national security advisor and national security advisor make efforts to ensure that the national cyber director is provided necessary interagency support.

[163] For example, Rob Joyce served under Homeland Security Advisor Tom Bossert for part of the Trump administration. Howard Schmidt and Michael Daniel served as cybersecurity coordinator in the Obama administration. Richard A. Clarke served as national coordinator for security, infrastructure protection, and counterterrorism in the Clinton administration. To take an example from another field, Gary Samore served as coordination for arms control and weapons of mass destruction in the Obama administration.

Bibliography

1947 National Security Act, Pub. L. No. 235, 61 Stat. 496 (1947). www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.

Alba, Davey. "How Russia's Troll Farm Is Changing Tactics before the Fall Election." *New York Times*, March 29, 2020. https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html.

Alexander, David. "Hagel, ahead of China Trip, Urges Military Restraint in Cyberspace." Reuters, March 28, 2014. www.reuters.com/article/us-usa-defense-cybersecurity-idUSBREA2R1ZH20140328.

———. "U.S. Reserves Right to Meet Cyber Attack with Force." Reuters, November 15, 2011. https://www.reuters.com/article/us-usa-defense-cybersecurity/u-s-reserves-right-to-meet-cyber-attack-with-force-idUSTRE7AF02Y20111116.

AP (Associated Press). "North Korean Programmer Charged in Sony Hack, WannaCry Attack." *PBS*, September 6, 2018. www.pbs.org/newshour/nation/north-korean-programmer-charged-in-sony-hack-wannacry-attack.

Arkin, William M. "Sunrise, Sunset." *Washington Post*, March 29, 1999. https://www.washingtonpost.com/wp-srv/national/dotmil/arkin032999.htm.

Authorization for Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224 (2001). https://www.congress.gov/107/plaws/publ40/PLAW-107publ40.pdf.

Axios. "NSA Director Says U.S. 'Disrupted a Concerted Effort to Undermine' 2018 Midterms." August 25, 2020. www.axios.com/nsa-director-foreign-interference-2018-midterms-d96f574d-c961-48b3-a7c9-8928f5a5decf.html.

Barnes, Julian E. "U.S. Cyber Command Expands Operations to Hunt Hackers from Russia, Iran and China." *New York Times*, November 2, 2020. https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

———. "U.S. Cyberforce Was Deployed to Estonia to Hunt for Russian Hackers." *New York Times*, December 3, 2020. www.nytimes.com/2020/12/03/us/politics/cyber-command-elections-estonia.html.

Barnes, Julian E., and Michael Venutolo-Mantovani. "Race for Coronavirus Vaccine Pits Spy Against Spy." *New York Times*, September 5, 2020. www.nytimes.com/2020/09/05/us/politics/coronavirus-vaccine-espionage.html.

BBC News. "North Korea 'Stole $2bn for Weapons via Cyber-Attacks.'" August 7, 2019. www.bbc.com/news/world-asia-49259302.

Bernard, Julie, and Mark Nicholson. "Reshaping the Cybersecurity Landscape: How Digitization and the COVID-19 Pandemic Are Accelerating Cybersecurity Needs at Many Large Financial Institutions." *Deloitte Insights*, July 24, 2020. https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

Bertrand, Natasha. "Biden Taps Intelligence Veteran for New White House Cybersecurity Role." *Politico*, January 6, 2021. www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508.

Board of Governors of the Federal Reserve System. "Designated Financial Market Utilities." Updated January 29, 2015. www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.

Borghard, Erica D. "U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace." Council on Foreign Relations, April 22, 2020. www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace.

Burt, Tom. "New Action to Combat Ransomware ahead of U.S. Elections." *Microsoft On the Issues* (blog), October 12, 2020. blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/.

Carter, Alexander L. "Improving Joint Interagency Coordination: Changing Mindsets." *Joint Force Quarterly 79* (2015): 19–26. https://ndupress.ndu.edu/Media/News/Article/621119/improving-joint-interagency-coordination-changing-mindsets/.

Chabrow, Eric. "White House Unveils Int'l Cybersecurity Strategy." Bank Info Security, May 17, 2011. www.bankinfosecurity.com/white-house-unveils-intl-cybersecurity-strategy-a-3645.

Cimpanu, Catalin. "A DDoS Gang Is Extorting Businesses Posing as Russian Government Hackers." *ZDNet*, October 24, 2019. www.zdnet.com/article/a-ddos-gang-is-extorting-businesses-posing-as-russian-government-hackers/.

———. "US Cyber Command Exposes New Russian Malware." *ZDNet*, November 1, 2020. www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/.

CISA (Cybersecurity and Infrastructure Security Agency). "Alert (AA20-106A): Guidance on the North Korean Cyber Threat." Last revised June 23, 2020. us-cert.cisa.gov/ncas/alerts/aa20-106a.

———. "Alert (AA20-006A): Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad." Last revised October 24, 2020. us-cert.cisa.gov/ncas/alerts/aa20-006a.

———. "Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector." Last revised November 2, 2020. us-cert.cisa.gov/ncas/alerts/aa20-302a.

———. "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Last revised March 16, 2018. us-cert.cisa.gov/ncas/alerts/TA18-074A.

———. "Automated Indicator Sharing (AIS)." Accessed February 19, 2021. us-cert.cisa.gov/essa.

———. "Critical Infrastructure Partnership Advisory Council." Accessed February 19, 2021. www.cisa.gov/critical-infrastructure-partnership-advisory-council.

———. "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI)." December 16, 2020. https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

Coats, Daniel R. *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*. Office of the Director of National Intelligence, January 29, 2019. www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Cohen, Zachary. "US Cyber Command Expands Operations against Russia, China and Iran." *CNN*, November 3, 2020. www.cnn.com/2020/11/02/politics/cyber-command-russia-china-iran/index.html.

Coleman, Kevin G. "Cyber Intelligence: DoD's Cyber Operations Strategy – Today and Tomorrow." BreakingGov, July 15, 2011. breakinggov.com/2011/07/15/cyber-intelligence-dods-operations-strategy-today-and-tomorr/.

Commission on the Theft of American Intellectual Property. *IP Commission 2019 Review: Progress and Updated Recommendations*. Washington, DC: National Bureau of Asian Research, February 2019. https://www.nbr.org/wp-content/uploads/pdfs/publications/ip_commission_2019_review_of_progress_and_updated_recommendations.pdf.

———. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*. Washington, DC: National Bureau of Asian Research, February 2017. http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. Arlington, VA: CNA, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Council of Europe. *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*. Strasbourg, France: Council of Europe, July 13, 2020. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

CSC (Cyberspace Solarium Commission). *CSC Report*. Arlington, VA: CSC, March 2020. https://www.solarium.gov/.

CSIS (Center for Strategic and International Studies). "Significant Cyber Incidents." Accessed February 22, 2021. www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cyber-Digital Task Force. *Report of the Attorney General's Cyber Digital Task Force*. Washington, DC: Department of Justice, July 2, 2018. https://www.justice.gov/archives/ag/page/file/1076696/download.

Demarest, Joseph. "Taking Down Botnets." Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism. Washington, DC: FBI, July 15, 2014. www.fbi.gov/news/testimony/taking-down-botnets.

DHS (Department of Homeland Security). *FY 2021 Budget in Brief*. Washington, DC: DHS, 2020. www.dhs.gov/sites/default/files/publications/fy_2021_dhs_bib_0.pdf.

DoD (Department of Defense). *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: DoD, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. *Summary: Department of Defense Cyber Strategy 2018*. Washington, DC: DoD, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

———. *Task Force on Cyber as a Strategic Capability: Executive Summary*. Washington, DC: DoD Defense Science Board, June 2018. https://dsb.cto.mil/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

———. *Task Force on Cyber Deterrence*. Washington, DC: DoD Defense Science Board, February 2017. https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

DOJ (Department of Justice). "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector." News release, March 24, 2016. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged#:~:text=A%20grand%20jury%20in%20the,Guard%20Corps%2C%20on%20computer%20hacking.

FBI (Federal Bureau of Investigation). "Iranians Charged with Hacking U.S. Financial Sector." March 24, 2016. www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.

———. "National Cyber Investigative Joint Task Force." Accessed January 19, 2021. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

Gallagher, Sean. "Australian Defense Firm Was Hacked and F-35 Data Stolen, DOD Confirms." *Ars Technica*, October 13, 2017. arstechnica.com/information-technology/2017/10/australian-defense-firm-was-hacked-and-f-35-data-stolen-dod-confirms/.

Garamone, Jim. "Esper Describes DOD's Increased Cyber Offensive Strategy." US Department of Defense, September 20, 2019. www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.

Gjelten, Tom. "Cyber Briefings 'Scare the Bejeezus' Out of CEOs." *NPR*, May 9, 2012. www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos.

Guardian. "China Theft of Technology Is Biggest Law Enforcement Threat to US, FBI Says." February 6, 2020. www.theguardian.com/world/2020/feb/06/china-technology-theft-fbi-biggest-threat.

GWU CCHS (George Washington University Center for Cyber and Homeland Security). *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: Center for Cyber and Homeland Security, October 2016. http://cchs.auburn.edu/_files/into-the-gray-zone.pdf.

Hannigan, Robert. *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre*. London: Royal United Services Institute for Defence and Security Studies, February 2019. https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf.

Hayden, Michael V. "The Making of America's Cyberweapons." *Christian Science Monitor*, February 24, 2016. www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0224/The-making-of-America-s-cyberweapons.

Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878.

Hearing on the Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace, Before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, 116th Cong. (2020). Statement of General Paul M. Nakasone, Commander United States Cyberspace Command. https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.

Henriksen, Anders. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): tyy009. https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865.

Hildreth, Steven A. *Cyberwarfare*. Washington, DC: Congressional Research Service, June 19, 2001. https://fas.org/sgp/crs/intel/RL30735.pdf.

Holohan, Meghan. "As the Morris Worm Turned." *The Link*. Accessed February 26, 2021. https://www.cs.cmu.edu/link/morris-worm-turned.

House of Representatives. *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Conference Report to Accompany H.R. 6395*. Washington, DC: Government Printing Office, 2020. https://docs.house.gov/billsthisweek/20201207/CRPT-116hrpt617.pdf.

John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. (2018). https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

Kaplan, Fred. "How the United States Learned to Cyber Sleuth: The Untold Story." *Politico Magazine*, March 20, 2016. www.politico.com/magazine/story/2016/03/russia-cyber-war-fred-kaplan-book-213746.

Kramer, Frank, Bob Butler, and Catherine Lotrionte. "Raising the Drawbridge with an 'International Cyber Stability Board.'" *The Cipher Brief*, March 4, 2019. https://www.thecipherbrief.com/raising-drawbridge-international-cyber-stability-board.

Kramer, Franklin D., and Robert J. Butler. *Cybersecurity: Changing the Model*. Washington, DC: Atlantic Council, April 2019. www.atlanticcouncil.org/wp-content/uploads/2019/04/Cybersecurity-Changing_the_Model.pdf.

Krebs, Christopher. "We Prepared for More Russian Interference. But This Year the Assault on Democracy Was from within the US." *CNN*, December 15, 2020. www.cnn.com/2020/12/15/opinions/assault-on-democracy-within-the-us-krebs/index.html.

Krebs, David. "At Least 30,000 U.S. Organizations Newly Hacked via Holes in Microsoft's Email Software." Krebs on Security, March 5, 2021. https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

Lee, Robert M. *The Sliding Scale of Cyber Security*. Bethesda, MD: SANS Institute, August 2015. https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240.

Liptak, Kevin. "John Bolton: US Is Going on the Offensive against Cyberattacks." *CNN*, September 20, 2018. www.cnn.com/2018/09/20/politics/us-cybersecurity-strategy-offense-john-bolton/index.html.

Lopez, Todd C. "Cyber Command Expects Lessons from 2018 Midterms to Apply in 2020." Joint Chiefs of Staff. Accessed March 22, 2021. www.jcs.mil/Media/News/News-Display/Article/1759176/cyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020/.

———. "For 2020 Election, Threat Is Bigger than Russia." US Department of Defense, August 8, 2020. www.defense.gov/Explore/News/Article/Article/2306001/for-2020-election-threat-is-bigger-than-russia/.

Lyngaas, Sean. "CISA Orders US Agencies to Address Microsoft Flaws Exploited by Suspected Chinese Hackers." *Cyberscoop*, March 3, 2021. https://www.cyberscoop.com/dhs-microsoft-exchange-flaws-patch-china/.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010. www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Martelle, Michael, ed. *Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War against ISIL*. Briefing Book No. 637. Washington, DC: National Security Archive, August 13, 2018. nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

———. *Joint Task Force – Computer Network Defense: 20 Years Later.* Briefing Book No. 677. Washington, DC: National Security Archive, June 29, 2019. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-06-29/joint-task-force-computer-network-defense-20-years-later.

Munsing, Evan, and Christopher J. Lamb. *Joint Interagency Task Force–South: The Best Known, Least Understood Interagency Success*. Washington, DC: National Defense University Press, 2011. https://ndupress.ndu.edu/portals/68/documents/stratperspective/inss/strategic-perspectives-5.pdf.

Murgia, Madhumita, and Anna Gross. "Inside China's Controversial Mission to Reinvent the Internet." *Financial Times*, March 27, 2020. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

Nakashima, Ellen. "Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections." *Washington Post*, October 23, 2018. https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html.

———. "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries." *Washington Post*, September 20, 2018. www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

National Cyber Director Act, H.R. 7331, 116th Cong. (2020). https://www.congress.gov/bill/116th-congress/house-bill/7331.

National Defense Authorization Act for 2017, Pub. L. No. 114–328, 130 Stat. 2000, Sec. 1654: Reports on Deterrence of Adversaries in Cyberspace (2016). https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf.

National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2020). www.congress.gov/bill/116th-congress/house-bill/6395.

NCSC (National Counterintelligence and Security Center). "Safeguarding Your Vote: A Joint Message on Election Security." October 6, 2020. https://www.dni.gov/index.php/ncsc-newsroom/item/2156-safeguarding-your-vote-a-joint-message-on-election-security.

NSA (National Security Agency). "Active Cyber Defense (ACD)." IAD Initiatives. Updated August 4, 2015. apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defense.cfm.

———."Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities." Cybersecurity Advisory, October 2020. media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF.

Nye, Joseph S., Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2017): 44–71. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

Obama, Barack. *Presidential Policy Directive 20 [Fact Sheet]*.Washington, DC: Office of the White House Press Secretary, January 2013. https://www.hsdl.org/?abstract&did=814897.

ODNI (Office of the Director of National Intelligence). "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." News release no. 29-20, August 7, 2020. www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncscdirector-william-evanina-election-threat-update-for-the-american-public.

ODNI CTIIC (Office of the Director of National Intelligence Cyber Threat Intelligence Integration Center). "Who We Are." Accessed January 19, 2021. https://www.dni.gov/index.php/ctiic-who-we-are.

ODNI NCTC (Office of the Director of National Intelligence National Counterterrorism Center). "History." Accessed March 2, 2021. https://www.odni.gov/index.php/nctc-who-we-are/history.

OSD (Office of the Secretary of Defense). *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress*. Washington, DC: Department of Defense, 2020. media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

Owens, Bill, producer. *60 Minutes*. Season 53, episode 13, "Securing the Election, the Last Slave Ship, James Corden." Aired November 29, 2020, on CBS. https://www.cbs.com/shows/60_minutes/video/3o1o_IfGRtl6jlZOLzSpBJ5l_eTodJEJ/11-29-2020-securing-the-election-the-last-slave-ship-james-corden/.

Paape, Josh. "Operation Eligible Receiver – The Birth Place of Cyber Security: Configurations." *Cyber Defense Magazine*, March 9, 2019. www.cyberdefensemagazine.com/operation-eligible-receiver-the-birth-place-of-cyber-security-configurations/.

Paganini, Pierluigi. "The Biggest Cyber-Security Incidents of 2016." Infosec Resources, January 3, 2017. resources.infosecinstitute.com/topic/the-biggest-cyber-security-incidents-of-2016/.

PCCIP (President's Commission on Critical Infrastructure Protection). *Critical Foundations: Protecting America's Infrastructures*. Washington, DC: PCCIP, October 1997. chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf.

Pomerleau, Mark. "New Authorities Mean Lots of New Missions at Cyber Command." Fifth Domain, May 8, 2019. www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.

———. "Two Years In, How Has a New Strategy Changed Cyber Operations?" Fifth Domain, November 11, 2019. www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.

———. "What New Documents Say about US-Partner Cyber Operations." Fifth Domain, January 23, 2020. www.fifthdomain.com/dod/2020/01/23/what-new-documents-say-about-us-partner-cyber-operations/.

Rosenzweig, Paul, Steven Bucci, and David Inserra. *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*. Washington, DC: The Heritage Foundation, May 5, 2017. https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown, 2018.

Sanger, David E., and Julian E. Barnes. "U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came." *New York Times*, November 9, 2020. www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.

Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." *New York Times*, January 2, 2021. www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." *New York Times*, June 15, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Schmidle, Nicholas. "The Digital Vigilantes Who Hack Back." *New Yorker*, April 30, 2018. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

Schrier, Rob. "A Case for Action: Changing the Focus of National Cyber Defense." *Cyber Defense Review* (Fall 2019): 23–26.

Smart, William. *Lessons Learned Review of the WannaCry Ransomware Cyber Attack*. London: UK Department of Health and Social Care, February 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

Smith, Brad. "A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response." *Microsoft on the Issues* (blog), December 18, 2020. blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

Smith, Zhanna Malekos, Eugenia Lostri, and James A. Lewis. *The Hidden Costs of Cybercrime*. San Jose, CA: McAfee (December 2020). www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Snyder, Charley, and Michael Sulmeyer. "Decoding the 2017 NDAA's Provisions on DoD Cyber Operations." *Lawfare* (blog), January 30, 2017. https://www.lawfareblog.com/decoding-2017-ndaas-provisions-dod-cyber-operations.

SSCI (US Senate Select Committee on Intelligence). *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media*. 116th Cong., 1st Sess., October 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Starks, Tim. "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says." *Politico*, September 10, 2020. www.politico.com/news/2020/09/10/russia-china-iran-cyberhack-2020-election-411853.

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. "Russia's Information Warfare: Exploring the Cognitive Dimension." *MCU Journal* 10, no. 2 (2019): 129–147. doi:10.21140/mcuj.2019100208.

USCYBERCOM (US Cyber Command). *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: DoD, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

———. "Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation." December 3, 2020. www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.

———."USCYBERCOM Fragord 01 to Taskord 16-0063 to Establish Joint Task Force (JTF)-Ares to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyberspace." May 2016. https://www.stratcom.mil/Portals/8/Documents/FOIA/FOIA%2017-023,%2017-033,%2017-064%20-%20USCYBERCOM%20Joint%20Task%20Force%20Areas.pdf?ver=2017-04-19-111941-797.

———. "U.S. Cyber Command History." Accessed February 23, 20201. www.cybercom.mil/About/History/.

US Northern Command. "The Posse Comitatus Act." September 23, 2019. https://www.northcom.mil/Newsroom/Fact-Sheets/Article-View/Article/563993/the-posse-comitatus-act/

Vavra, Shannon. "Cyber Command Deploys Abroad to Fend off Foreign Hacking ahead of the 2020 Election." *CyberScoop*, August 25, 2020. www.cyberscoop.com/2020-presidential-election-cyber-command-nakasone-deployed-protect-interference-hacking/.

———. "Here's What John Bolton Had to Say about Cybersecurity Policy in His New Book." *CyberScoop*, June 22, 2020. www.cyberscoop.com/john-bolton-book-cybersecurity-nspm-13-crowdstrike/.

White House. *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*. Washington, DC: The White House, May 22, 1998. https://fas.org/irp/offdocs/paper598.htm.

———. "The Comprehensive National Cybersecurity Initiative." Accessed February 23, 2021. obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

———. "FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment." Washington, DC: The White House, Office of the Press Secretary, December 29, 2016. obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

———. "FACT SHEET: President Xi Jinping's State Visit to the United States." Washington, DC: The White House, Office of the Press Secretary, September 25, 2015. obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

———. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: The White House, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. *National Cyber Strategy of the United States of America*. Washington, DC: The White House, September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

———. *National Security Directive 42 (NSD-42): National Policy for the Security of National Security Telecommunications and Information Systems*. Washington, DC: White House Office, July 5, 1990. www.hsdl.org/?abstract&did=458706.

———. *National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD 23.* Washington, DC: The White House, January 8, 2008. fas.org/irp/offdocs/nspd/nspd-54.pdf.

———. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House, February 2003. https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

———. *Presidential Policy Directive -- United States Cyber Incident Coordination*. Washington, DC: The White House, July 26, 2016. obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

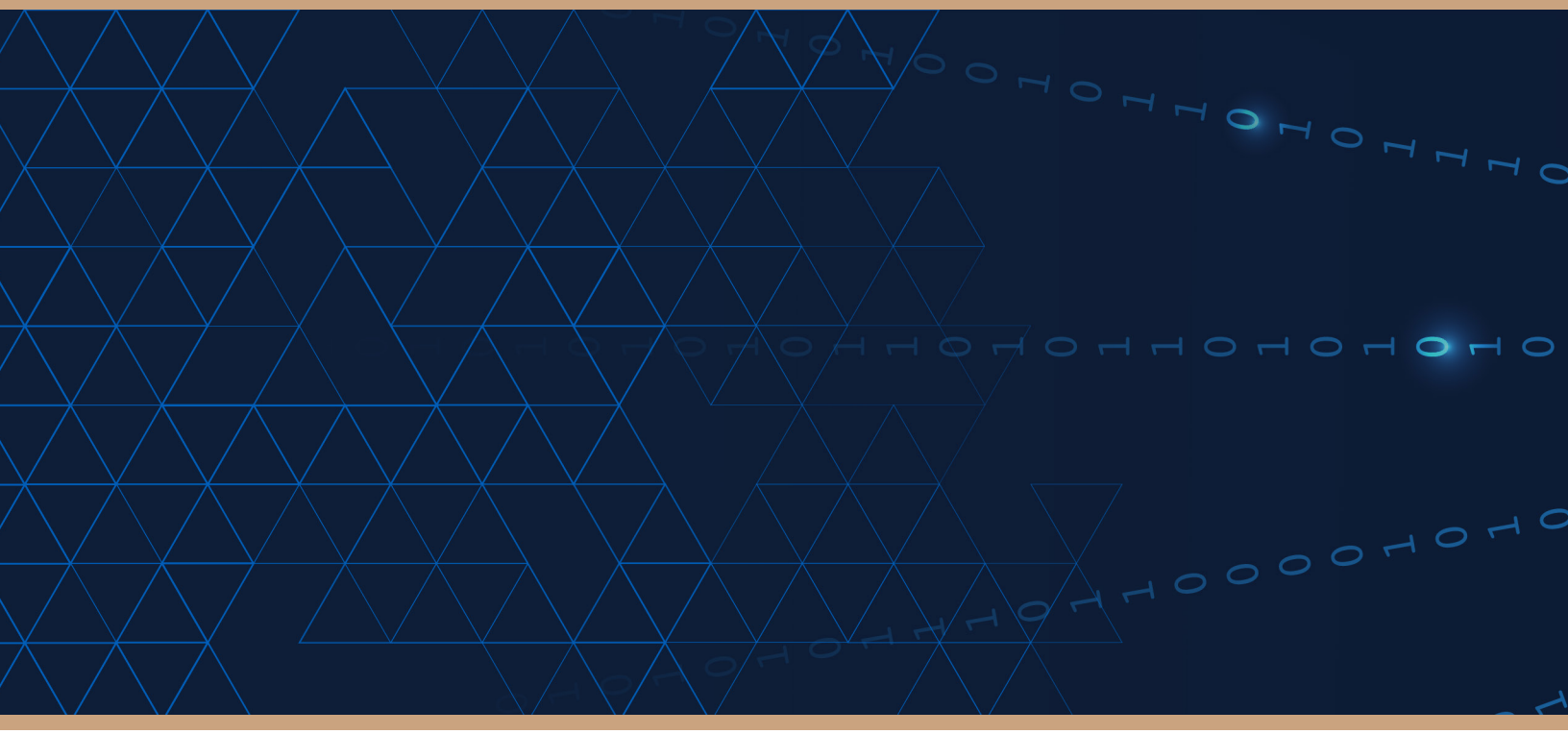
Acknowledgments

This report was made possible by support from APL, where the authors serve as a senior fellow (Miller) and consultant (Butler). The authors particularly thank APL's Christine Fox, Matt Schaffer, and Donna Gregg for their support and guidance. Jen Easterly, Chris Inglis, Rob Schrier, Paul Stockton, and Kiersten Todt all provided invaluable comments and suggestions. The authors also thank participants in a January 2020 workshop held at the APL campus: Bob Blunden, Tom Bossert, Terry Burruss, John Carlin, David Cohen, Dennis Crall, John Felker, Christine Fox, Charles Garzoni, Emily Goldman, Avril Haines, Chris Inglis, Dave Lacquement, David Luber, Anne Neuberger, Maegen Nix, Rob Schrier, Paul Stockton, Michael Sulmeyer, Angela Thompson, Stony Trent, and Ed Wilson.

About the Authors

Dr. James N. Miller is president and chief executive officer of Adaptive Strategies, LLC. He is known for his expertise and leadership in nuclear deterrence, missile defense, space policy, and cyber warfare. As under secretary of defense for policy from 2012 to 2014, Dr. Miller served as the principal civilian advisor to the secretary of defense on strategy, policy, and operations, working to strengthen relations with allies and partners in Europe, the Middle East, and Asia and to reduce the risks of miscommunication with Russia and China. He served as principal deputy under secretary of defense for policy from 2009 to 2012.

Robert J. Butler serves as the managing director for Cyber Strategies LLC, a full-service cybersecurity and risk management firm for public and private sector clients. Mr. Butler has a distinguished career in information technology, intelligence, and national security in both the public and private sectors as well as nationally and internationally. He is a retired US Air Force colonel and a former member of the Defense Department's Senior Executive Service, and he served as the first deputy assistant secretary of defense for cyber and space policy.



JOHNS HOPKINS
APPLIED PHYSICS LABORATORY