Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

CYBER AND DETERRENCE

The Military-Civil Nexus in High-End Conflict

Franklin D. Kramer, Robert J. Butler,
and Catherine Lotrionte

CYBER AND DETERRENCE

The Military-Civil Nexus in High-End Conflict

Franklin D. Kramer, Robert J. Butler,
and Catherine Lotrionte

Cover photo credit: US Navy/WikiCommons, US Air Force/WikiCommons, Patrick Finnegan/Flickr.

ISBN: 978-1-61977-457-5

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

January 2017

TABLE OF CONTENTS

INTRODUCTION

This paper analyzes cyber's role in deterrence and defense—and specifically the military-civil nexus and the relationship between the Department of Defense (DoD), the civil agencies, and the key private operational cyber entities, in particular the Internet Service Providers (ISPs) and electric grid operators. The focus of the paper is on high-end conflict including actions by an advanced cyber adversary, whether state or nonstate, and not on the "day-to-day" intrusions and attacks as regularly occur and are generally dealt with by governmental agencies and the private sector without military involvement. High-end conflict can be expected to include attacks within the United States homeland as well as in forward theaters.

Last year, the Barack Obama administration issued PPD-41, "Cyber Incident Protection," setting forth cyber security incident roles and missions for federal agencies but with no explicit reference to the Department of Defense.[1] By contrast, the *DoD Cyber Strategy* provides that DoD will be prepared to "defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence."[2] Certainly, in a conflict where an adversary will utilize cyber as part of an overall military attack, the DoD will necessarily play a major operational role. This paper discusses what that role should entail.

In a high-end conflict, the military will rely heavily on the availability of the telecommunication and electric grid networks, and those networks—including those abroad—will likely need assistance from the military to remain operationally effective. Understanding cross-sectoral dependencies and potential cascading effects from attacks will be crucial. Accordingly, to achieve deterrence and/or successful defense with respect to such a conflict or potential conflict situation, particularly against high-end cyber adversaries, the military, civil authorities, the ISPs, and grid operators will need to work closely together both prior to and during the conflict. This will be true both inside the United States and in the forward theaters where conflict is likely to occur.

. . . [M]ilitary, civil authorities, the ISPs, and grid operators will need to work closely together . . . both inside the United States and in the forward theaters. . .

This paper is organized in two parts. The first, and more extensive section, focuses on requirements necessary inside the United States. The second discusses requirements for forward theaters, building on the analysis for the US territory and the authors' previous paper "Cyber, Extended Deterrence, and NATO."[3] The broad conclusion of the paper is that effective planning and operations require two overlapping sets of requirements to be undertaken:

- The military needs to develop a concept of operations that allows it to determine the required support from the ISPs and the electric grid in a high-end contingency (such as defense of the Baltics) and to provide the basis for a prioritized approach to cyber protection, resilience, and recovery of those networks. To prioritize mission-essential networks and industrial control systems that are critical for responding to regional crises, coordination with civil authorities, the ISPs, and electric grid operators both prior to and during a crisis will be necessary.
- The civil authorities, the ISPs, and electric grid operators need to develop contingency planning to elucidate the type of assistance they are likely to need from the military to provide the protection, resilience, and recovery necessary to maintain adequate telecommunications and grid operations for the nation in the event of a high-end contingency. The grid and ISP operators have unique knowledge of their specific system architectures and restoration plans; therefore, they are the best experts to convey that information to the military so the military is ready to actively

[1] Presidential Policy Directive/PPD 41, "US Cyber Incident Coordination," The White House Press Office, July 26, 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. See also US Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 30, 2016, https://www.us-cert.gov/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf. The draft National Cyber Incident Response Plan, which will implement PPD-41, contains references to defense activities, but places DHS and other agencies in the lead even in the event of a significant cyber incident.

[2] US Department of Defense, *DOD Cyber Strategy* (Washington, DC: US Government, 2015), 14, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[3] Franklin D. Kramer, Robert J. Butler, and Catherine Lotrionte, "Cyber, Extended Deterrence, and NATO," Atlantic Council, 2016, http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf.

support their efforts both during an attack and for post-cyberattack restoration. Without this foreknowledge about the specific systems, DoD personnel who undertake to assist during a crisis would be ineffective and could in fact cause harm to the systems and contribute to other adverse consequences.

To accomplish these objectives in the United States, six steps need to be undertaken:

1. First, contingency plans for military, civil authority, ISP, and electric grid operator interactions must be established for a high-end contingency through the use of an effective planning process supported by regular exercises and detailed playbooks that are routine in other emergency scenarios such as storms, fires, and earthquakes.

2. Second, clear chains of command for a high-end contingency need to be established between the civil authorities and the DoD and within the DoD itself, and an operational mechanism needs to be created to include the ISPs and the electric grid to allow prompt and responsive actions. To remedy existing disconnects between the DoD and other departments and to allow for proper interaction with the ISPs and grid operators in the context of a high-end contingency, Congress should consider creating a requirement for "unified cyber actions" along the lines of what the Goldwater-Nichols Act established for the DoD, requiring joint actions among the four services for war-fighting purposes.

3. Third, it is important to undertake actions in advance of a high-end attack to establish the greatest likelihood of effective protection, resilience, and recovery, as numerous analyses have determined that to generate desired results defenders cannot wait for the actual attack. Among other important steps prior to conflict, intrusions need to be blocked as much as possible; malware needs to be removed; and capabilities for maintaining data integrity, confidentiality, and availability need to be built and exercised. Critical to this effort is the use of a variety of adaptive resilience techniques, ranging from diversity and redundancy to moving target defenses and deception.[4] All these resiliency features require development and implementation prior to conflict. Not all attacks can be protected against, but their effects can be mitigated if steps are taken in advance. DoD can utilize the knowledge generated in the defense of its own networks to assist defenders, and undertake research and development through the Defense Advanced Research Projects Agency and other DoD applied research and development activities to provide advanced capabilities.

4. Fourth, the roles of the National Mission Teams (NMTs), and the associated National Guard–supported teams, currently being established by Cyber Command to respond to cyberattacks of significant consequence, must be developed and clarified. NMTs and National Guard missions during an attack should be developed, specifying how they will interact with ISPs and grid operators. NMTs and the National Guard will not have the degree of expertise that ISP and grid operators have in their respective domains, but a combined effort utilizing exercises and modeling can establish tactics, techniques, and procedures for operating in a degraded environment. Additionally, NMTs and the National Guard should operate not only once a high-end attack has begun, but should help support actions prior to such an attack that will enhance protection, resilience, and recovery of the ISPs and the electric grid if an attack occurs. In addition to substantive planning, operational legal authorities must be clarified before an attack occurs. Moreover, a determination should be made whether the capabilities of the active force and the National Guard are sufficient or whether they need to be supplemented by private sector cyber security expertise, working under government direction and control in connection with high-end contingencies or in direct support to the ISPs and grid operators. For both conflict and restoration operations, such private sector skilled personnel may be necessary, especially if the NMTs and National Guard are needed to give direct support to DoD in a time of crisis. Any private sector personnel will need to be familiar with the specific operational technology networks, software applications, and protocols of the specific critical infrastructure.

5. Fifth, DoD should establish programs and funding to support resilience and recovery. The US government should leverage the Defense Production Act to ensure that readiness reserves in hardware and systems exist for critical infrastructure providers as they reconstitute/recover.[5] The DoD could provide a contractual

[4] Harriet G. Goldman, *Building Secure, Resilient Architectures for Cyber Mission Assurance* (The MITRE Corporation, 2010), https://www.mitre.org/sites/default/files/pdf/10_3301.pdf.

[5] Melissa E. Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," Chap. 6 in Nicholas Burns and Jonathon Price (eds.), *Securing Cyberspace: A New Domain for National*

program for the purchase of key infrastructure components. Companies who participate could be further incentivized through payments and limited liability protection to provide greater levels of security to their industry supply chain and vendor management processes and to adopt best-practice secure engineering and better-engineered products.[6] DoD funding could also support the Department of Energy efforts contemplated under the Strategic Transformer Reserve of the Fixing America's Surface Transportation Act (FAST Act).[7]

6. Sixth, offense will be a key element of effective operations. Prior to conflict, it will be important to undertake expanded "fusion" efforts, largely by civil authorities, to bring to bear intelligence, cyber, financial, law enforcement, and other capabilities to disrupt adversarial cyber planning and operations. Campaign planning should include courses of action to respond to so-called hybrid warfare, including cyber-enabled "flexible deterrent (and response) options," so that commanders will have a full spectrum of options to utilize if the president determines it appropriate. In the event of conflict, cyber capabilities can be used against an adversary, targeting not only adversary cyber but also military capabilities such as sensors, communications, logistics, and military supporting infrastructures.

In forward theaters, effective operations will require all of the foregoing to be undertaken including contingency planning; clear delineation of command chain; clarity on the role of cyber teams; identification of prior actions to enhance protection, resilience, and recovery; and use of offense. However, as the United States will be operating as part of an alliance or organized coalition, cyber requirements will have to be coordinated and undertaken with allies and coalition partners. Accordingly, in addition to the specifics noted above, three additional elements will be key: the United States should act as a "cyber framework nation" to help support national capabilities; operational partnerships should be created between and among the military, civil authorities, the ISPs, and grid operators in the host nation; and cyber tools should be part of the military war-fighting effort, to disrupt adversary cyber operations and military capabilities including sensors, communications, logistics, and war-supporting critical infrastructure.

I. THE CURRENT THREAT CONTEXT

A starting point for analysis is to recognize that in conflict or prior to conflict, and focusing on deterrence and readiness, cyber is only a part of the overall picture. As Secretary of Defense Ashton Carter has stated the United States and its allies and partners face five key military or potential military challenges: 1) Russia, particularly facing NATO in the east; 2) North Korea, with the US deterrent encompassing its treaty allies of both the Republic of Korea and Japan; 3) the Gulf, where the Gulf Cooperation Council countries are subject to Iranian threat; 4) the continuous violent activities of the Islamic State of Iraq and al-Sham (ISIS) and al-Qaeda; and 5) the increasingly competitive and complex actions of China in the East and South China Seas.[8] As the Department of Defense's (DoD's) 2015 Cyber Strategy has set forth, each of these threat or potential threat actors has cyber capability—Russia and China at high-capability levels; Iran and North Korea somewhat lower; and the ISIS/al-Qaeda capability harder to determine, though they clearly make use of the cyber realm.[9]

The risk to critical infrastructure is substantial. According to Director of National Intelligence James Clapper, both the telecommunications sector and the electric grid face escalating cyber threats to their information technology and industrial control systems and other operational technology systems on which they rely.[10] Likewise, Admiral Michael Rogers, who is both commander of US Cyber Command and director of the National Security Agency, has testified "we have seen cyber actors from more than

Security (Queenstown, MD: Aspen Institute, February 2012).

[6] The Civil Reserve Air Fleet Program (CRAF) in fact provides for DoD inspections to ensure that appropriate engineering and maintenance standards are met.

[7] *Fixing America's Surface Transportation Act, P.L. 114-94*, (Washington, DC: United States Government Printing Office, December 4, 2015), hereinafter "the FAST Act," https://www.gpo.gov/fdsys/pkg/PLAW-114publ94/pdf/PLAW-114publ94.pdf.

[8] See Lisa Ferdinando, "Carter Outlines Security Challenges, Warns against Sequestration," DoD News, March 17, 2016, http://www.defense.gov/News-Article-View/Article/696449/carter-outlines-security-challenges-warns-against-sequestration. See also, "Opening Statement to Worldwide Threat Assessment Hearing," Senate Armed Services Committee, 114th Congress, (2015) (testimony of The Honorable James R. Clapper, Director of National Intelligence—"We must be prepared for a catastrophic large-scale cyber strike. . . . Russia, China, North Korea, and Iran, are all potential adversaries, who, if they choose, can do great harm."

[9] US Department of Defense, *DoD Cyber Strategy*, 9; see also Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: US Department of Defense, December 2013).

[10] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Committee," Office of the Director of National Intelligence, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

The California Independent System Operator (ISO) is one of the facilities of the seventy-four balancing authorities that balances supply and demand in the North American grid. According to Director of National Intelligence James Clapper, both the telecommunications sector and the electric grid face escalating cyber threats. *Photo credit*: Max Whittaker/*New York Times*/Redux.

one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing."[11] Several recent analyses have identified vulnerabilities of the Internet Service Providers (ISPs) to include distributed denial of service (DDOS) attacks, vulnerabilities in network devices, and insider threats.[12] Telecommunications systems have been attacked in Poland and Norway.[13]

In December 2015, the Ukraine electric grid was attacked,[14] disabling three distribution utilities and affecting up to 225,000 customers for several hours.[15] While there have been no reports of outages tied to cyberattacks in the United States, officials have expressed increased concern about cybersecurity threats to the power grid and the ability of state adversaries to cause large-scale damage to the US power grid.[16] Local power distribution assets are vulnerable to cyberattacks and there are long replacement and recovery times for these assets; damages from an attack could cause significant disruption.[17] One government study concluded

[11] Admiral Michael S. Rogers, "Statement before the Subcommittee on Emerging Threats and Capabilities," House Armed Services Committee, March 16, 2016, http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

[12] Kaspersky Lab, *Threat Intelligence Report for the Telecommunications Industry* (2016), 4, https://securelist.com/files/2016/08/Kaspersky_Telecom_Threats_2016.pdf. See also, *2016 Data Breach Investigations Report*, Rep. Verizon, June 6, 2016.

[13] Poland: Marcin Goettig, "Poland's No.2 Telecom Netia Says Suffered Cyber Attack," Reuters, July 8, 2016, http://www.reuters.com/article/us-poland-netia-cybercrime-idUSKCN0ZO22K; Norway: "Extent of Cyber Attacks Revealed," News in English, July 9, 2014, http://www.newsinenglish.no/2014/07/09/extent-of-cyber-attacks-revealed/.

[14] See SANS and E-ISACE, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (March 2016), http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar2016.pdf; DHS-Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack against Ukrainian Critical Infrastructure, Alert (IR-ALERT-H-16-056-01)," February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01; Kim Zetter, "Everything We Know about Ukraine's Power Plant Hack," *Wired*, January 20, 2016.

[15] SANS and E-ISACE, *Analysis of the Cyber Attack on the Ukrainian Power Grid*.

[16] Written statement of testimony of Caitlin Durkovich, Committee on Transportation and Infrastructure Subcommittee on Economic Development, Public Buildings and Emergency Management, April 14, 2016, 2 ("A targeted cyber incident – either alone or combined with a physical attack – on the power system could lead to huge costs and cascading effects, and sustained outages over large portions of the electric grid and prolonged disruptions in communications, water and wastewater treatment services, health care delivery, financial services, and transportation."); See also, North American Electric Reliability Corporation, *Cyber Attack Task Force: Final Report* (Washington, DC: North American Electric Reliability Corporation, 2012), 20-23, http://www.nerc.com/%20docs/cip/catf/12-CATF_FINAL_REPORT_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf; Jamie Crawford, "The U.S. Government Thinks China Could Take Down the Power Grid," CNN Politics, CNN, November 21, 2014.

[17] Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," CNN, September 26, 2007,

that if as few as nine of the fifty-five thousand distribution substations in the United States were taken offline, coast-to-coast blackouts could result.[18] In 2014, the Department of Homeland Security (DHS) warned utilities that the BlackEnergy malware "has compromised numerous . . .[industrial control systems]."[19] Likewise, Admiral Rogers has testified, "We have also observed that energy firms and public utilities in many nations including the United States have had their networks compromised by state cyber actors."[20]

As the attacks noted above and as many additional well-known cyber intrusions have demonstrated, there are substantial vulnerabilities in the cyber arena for adversaries to exploit.[21] Those vulnerabilities present an inviting target and can reduce the effectiveness of other actions by the United States and its allies and partners to deter, or if necessary defend and prevail in, conflict. In a high-end conflict, the almost certain likelihood is that cyberattacks would be multiple and repeated. As the Homeland Security Advisory Council recently stated:

> "Unless APTs [advanced persistent threats] are completely eradicated from communications, financial and electric grid networks, that malware will continue to disrupt restoration operations and create further cascading infrastructure failures and system instability. . . [Cyber security] capabilities should account for this risk of re-attack."[22]

Most obviously in a network-centric world, vulnerabilities in the cyber domain can have cascading effects of highly negative consequence for military operations as well as for the nation. Thus:

> "[A]dversaries may launch simultaneous attacks on the electric, communications, and financial sectors. Such multi-sector attacks (and the cascading failures they would produce) compound problems for infrastructure restoration."[23]

In particular, militaries rely heavily on telecommunications and the electric grid for intelligence, operations, logistics, and communications—and, at the strategic level, allies and partners have the same dependencies. In 2008, the Defense Science Board concluded that the "[a]lmost complete dependence of military installations on a fragile and vulnerable commercial power grid and other critical national infrastructure places critical military and Homeland defense missions at an unacceptable high risk of extended disruption."[24] The Senate Armed Services Committee found "approximately 50 successful intrusions" in a one-year period into contractor networks supporting US Transportation Command and that such "intrusions . . . posed a threat to U.S. military operations."[25] Deputy Secretary of Defense Robert Work has stated that "almost all our combat power" is in the United States and "you now have to assume that you're going to be under intense cyber attack even before you move."[26]

In a conflict, vulnerable cyber dependencies will provide an inviting, and almost inevitable, target for adversaries. Moreover, as the United States strategy plans to provide security for and, if necessary, fight forward with allies and partners in the arenas noted above, it becomes an essential part of US strategy to enhance deterrence for itself and for allies and partners in the cyber arena. As Admiral Rogers has testified:

> "[I]f we cannot defend the infrastructure that undergirds our DoD bases and forces from foreign-based cyber threats, then our nation's military capabilities are weakened and all our instruments of national power diminished. That

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews.

[18] Rebecca Smith, "U.S. Risks National Blackout from Small-Scale Attack," *Wall Street Journa*l, March 12, 2014, http://www.wsj.com/articles/SB10001424052702304020104579433670284061220.

[19] US Department of Homeland Security, Industrial Control Systems, Cyber Emergency Response Team, ALERT-14-281-01B): "Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," December 10, 2014, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[20] Admiral Michael S. Rogers, Commander, United States Cyber Command, "Statement before the Senate Committee on Armed Services," United States Senate Committee on Armed Services, September 29, 2015, http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf.

[21] See James R. Clapper, "Statement for the Record: Worldwide Cyber Threats, House Permanent Select Committee on Intelligence," Office of the Director of National Intelligence, September 10, 2015, https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.

[22] Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I - Incident Response* (June 2016), 7, https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

[23] Ibid., 9.

[24] Report of the Defense Science Board Task Force on DoD Energy Strategy, *More Fight-Less fuel* (Washington, DC: US Department of Defense, February 2008), http://www.acq.osd.mil/dsb/reports/ADA477619.pdf.

[25] Senate Armed Services Committee, "Inquiry into Cyber Intrusions Affecting U.S. Cyber Command Contractors (2014)," 2014, viii, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

[26] Bradley Peniston, "Work: 'The Age of Everything Is the Era of Grand Strategy,'" *Defense One*, November 2, 2015, http://www.defenseone.com/management/2015/11/work-age-everythingera-grand-strategy/123335/.

> leaves our leaders with a need for additional options to pursue short of open hostilities, and with fewer capabilities in an actual clash of arms. This raises risk for all by inviting instability and miscalculation."[27]

At home and in each of the theaters mentioned, the United States needs to provide deterrence by supporting enhanced defense and resilience for itself, its allies, and its partners through an active role in helping defend critical national networks, most particularly the military, telecoms, and the electric grid.

The Department of Defense has a key role in accomplishing that task. Under current US strategy, the DoD is responsible for its own networks and must also "be prepared to defend" against "cyberattacks of significant consequence"[28] in the United States. Significant attacks in conflict against critical infrastructure would meet that criterion. The key issue, discussed below, is what is necessary for the DoD effectively to be "prepared to defend."

II. THE NEED FOR ENHANCED CIVIL-MILITARY COORDINATION

Civil-military coordination is critical to the protection and resilience of both the telecom and electric grid networks. There are ongoing substantial efforts by the US government (USG) and the private sector to generate such results. These efforts include the administration's recent Presidential Policy Directive 41 (PPD-41),[29] the Cybersecurity National Action Plan,[30] and the Cybersecurity Information Sharing Act.[31] Sector-specific programs such as the Cybersecurity Risk Information Sharing Program (CRISP)[32] and the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2)[33] focused on the electric grid are steps in the right direction in facilitating public-private partnerships, but they currently do not include DoD. Rather, as set forth below, current coordination does not reach the level to assure effective operations in the event of a high-end conflict. The government and key private sector actors—telecom and grid operators—need to enhance their cooperation, particularly focused on greater actions by the Department of Defense.

A. The ISPs Have Requested Government Direction for High-End Conflict

The National Security Telecommunications Advisory Committee (NSTAC) is composed of executives from the telecommunications industry and provides recommendations to the president. In its *Report to the President on Information and Communications Technology Mobilization*, the NSTAC concluded that for high-end conflict (which it characterized as state "RED"), industry alone could not meet all national security requirements and government direction was required. The report stated:

> "RED: At this level, industry is unable to fully mitigate the incident, even with additional authorities. If the incident cannot be fully mitigated, industry would want recommendations or direction on the priorities for protection (e.g., pre-incident) or recovery (e.g., post-incident). Specification of national security priorities is a responsibility inherent to Government."[34]

[27] Written Statement of Testimony of Admiral Rogers, Senate Committee on Armed Services, September 29, 2015, https://www.hsdl.org/?view&did=792559.

[28] US Department of Defense, The *DoD Cyber Strategy,* 5. ("For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence. While cyberattacks are assessed on a case-by-case and fact-specific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.")

[29] Presidential Policy Directive, "United States Cyber Incident Coordination," (PDD-41), July 26, 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[30] The White House, Office of the Press Secretary, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[31] Cybersecurity Act of 2015, H.R. 2029, 114th Congress, Pub. L. 114-113, December 18, 2015. Although the act provides useful liability protection for companies that share information with DHS, under the current procedures there is no liability protection for companies if they share information with other federal government agencies such as DoD or DOE. One recommendation would be to amend the act expanding the protection currently granted within the act for sharing information with DHS to other government agencies.

[32] See written statement of testimony of Patricia A. Hoffman, Committee on Transportation and Infrastructure Subcommittee on Economic Development, Public Buildings, and Emergency Management, April 14, 2016, 3. CRISP is a public-private partnership co-funded by DoE and industry to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. This is a valuable tool for coordinated information flows.

[33] Ibid. C2M2 is a DoE-industry developed model to improve cyber-security capabilities and to help private sector owners and operators better assess cybersecurity posture of the energy sector. The model provides an evaluation tool that helps organizations evaluate, prioritize, and improve cybersecurity capabilities.

[34] National Security Telecommunications Advisory Committee,

However, while the need for government direction in connection with high-end attacks is clear,[35] the NSTAC further concluded that there currently is no arrangement between government and industry for providing such direction:

> "As noted in the foundational findings, there is currently no protocol for the Government to convey in advance the national cyber priorities for protection, reconstitution, or recovery in the event an incident surpasses industry's mitigation ability."[36]

The importance of such interaction with the government was underscored by the NSTAC:

> "At this level, highly cyber-dependent organizations from industry and Government could experience degradation resulting in catastrophic impacts to our national security, economic security, public health and safety. Since the RED stage of cyber emergency is intended to describe the truly severe degradation of the national ICT [information and communications technology] base, the expectation is that, at that level, if it is ever achieved, the Nation would essentially be operating on a catastrophic or continuity-of-government footing. Accordingly, at that point, industry would seek to support Government initiatives to defend and preserve the Nation."[37]

Finally, the NSTAC noted the need for effective government direction that could be provided in a timely fashion for high-end conflict:

> "At the ORANGE or RED levels, the NSTAC considers it essential that for any coordination or communication with the Federal Government, the Government liaison to the ICT Confederation be empowered to make decisions and clearly and confidently commit resources or actions. The engaging Federal official may vary depending on the nature of the incident and could be from DHS, DOD, the Federal Bureau of Investigation/[Department of Justice], or the White House. In any case, the Federal official would speak on behalf of and, to the extent constitutionally permitted, with the authority of the Cabinet-level official they are representing. This authority is critical to ensure timely, effective response and the commitment of resources and other assistance."[38]

B. The Electric Grid Currently Lacks Adequate Protection and Resilience in the Event of a High-End Conflict, and Greater Coordination with the Government Is Required

It is well recognized that the electric grid is highly vulnerable to cyberattack. For example, testimony by a DHS official in 2016 stated:

> "A targeted cyber incident—either alone or combined with a physical attack—on the power system could lead to huge costs and cascading effects, with sustained outages over large portions of the electric grid and prolonged disruptions in communications, water and wastewater treatment services, health care delivery, financial services, and transportation."[39]

The National Research Council (NRC) similarly found in a 2012 study that:

> "Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, to date international terrorists have

Report to the President on Information and Communications Technology Mobilization (November 2014).

[35] Ibid., 13 ("Finding: The RED level conceptually represents a cyber emergency of the severest nature and greatest potential impact. At this level, the total commitment of industry to sustain network and system operations will be insufficient to meet the national need. Accordingly, Government will be expected to convey priorities and industry will do all that is possible to support national survival, under Government direction and within a comprehensive, legal, and operational framework.")

[36] Ibid., 12.

[37] Ibid., 12-13.

[38] Ibid., 21-22.

[39] Testimony of Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate, US Department of Homeland Security, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings and Emergency Management, US House of Representatives (April 2016), http://transportation.house.gov/uploadedfiles/2016-04-14-durkovich.pdf.

> shown limited interest in attacking the U.S. power grid. However, that should not be a basis for complacency. Since all parts of the economy, as well as human health and welfare, depend on electricity, the results could be devastating."[40]

The NRC further stated:

> "An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold.*
>
> "The largest power system disruptions experienced to date in the United States have caused high economic impacts. Considering that a systematically designed and executed terrorist attack could cause disruptions that were even more widespread and of longer duration, it is no stretch of the imagination to think that such attacks could entail costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product (GDP), which is currently about $12.5 trillion."[41]

In its GridEx III exercise report, the North American Electric Reliability Corporation (NERC) reported that participants in the exercise found that to be able to respond to crisis events, improved coordination during emergency situations between electric grid operations and the government was required to "resolve cyber threats and malware."[42] The report stated:

> "Industry needs to coordinate with government to identify and assess the cyber risks, likely by visiting the affected facilities. Unlike how industry responds to major storms through mutual assistance, industry's capability to analyze malware is limited and would require expertise likely available from software suppliers, control system vendors, or government resources. Electricity system recovery and restoration would be delayed or may not begin until the nature of the cyber risks are understood and mitigation strategies are available."[43]

Gerry Cauley, the CEO of NERC, has testified on the need for planning and coordination:

> "However, given the evolving threats to the BPS [bulk power system], we must remain vigilant. Grid Ex III showed that there is more that we can and should do to be better positioned to plan for and respond to a disruption of service upon which we all depend. This is a big job that involves everyone at the table today and many more."[44]

C. Civil Authorities and Private Sector Capabilities Are Not Sufficient to Meet the Requirements of a High-End Attack

The federal civil authorities have not undertaken to deal with a high-end attack by a capable adversary. PPD-41 on "Cyber Incident Protection" does not reference the Department of Defense. The PPD creates an interagency set of arrangements, and the draft National Cyber Incident Response Plan[45] essentially assumes that the cyberattacks contemplated would not necessarily require significant DoD involvement. However, in a military conflict against a capable adversary that will likely include higher-end cyberattacks against critical infrastructure, a leading role for DoD will be necessary and therefore must be planned for in advance. The Homeland Security Advisory Council, in a recent report, recognized the problems of managing a high-end attack and identified "the primary gaps" as:

> "• The lack of a fundamental framework and process methodology on the part of government to support and sustain infrastructure in the event of circumstances that arise to the orange and red CyberCon

[40] National Research Council, *Terrorism and the Electric Power Delivery System* (2012), 1.

[41] Ibid.

[42] NERC, *GridEx III Report* (March 2016), 15.

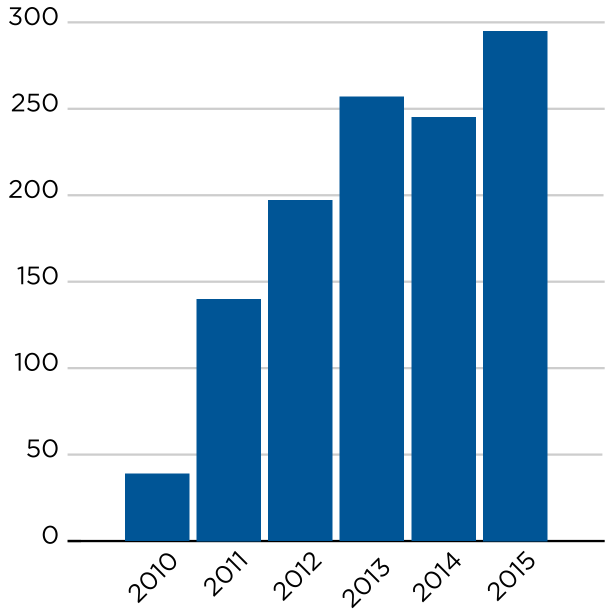
[43] Ibid., 15. See also Testimony of Gerry Cauley, President and Chief Executive Officer North American Electric Reliability Corporation, Before the Senate Energy and Natural Resources Committee (April 10, 2014), http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=9e67fb23-4235-4f20-bba8-c922fbd0205a.

[44] Testimony of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation House Transportation and Infrastructure Committee, Subcommittee on Economic Development, Public Buildings, and Emergency Management (April 14, 2016), http://www.nerc.com/news/testimony/Testimony%20and%20Speeches/Gerry%20Cauley%20Testimony%20-20April%2014%20House%20Transportation%20subcommittee%20hearing.pdf.

[45] US Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 30, 2016, https://www.uscert.gov/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf.

DARPA's Cyber Grand Challenge Final Event, the world's first all-machine cyber hacking tournament, on August 4, 2016 in Las Vegas. *Photo credit*: Defense Advanced Research Projects Agency.

Figure 1. Number of Reported Incidents, 2010-15



Source: Industrial Control Systems Cyber Emergency Response Team, which provides annual reports on the number of instances of cyberattacks on industrial control systems.

levels as outlined in the ICT Mobilization report which would require potentially new authorities and closer collaboration between government and industry beyond existing methodologies and may involve cross-sectoral efforts to mitigate the attack.

• A related inability for government to prioritize critical 'systems and assets' that could lead to a national cyber level incident and the need for a more robust industry/government dialog on priorities for the communications sector and protocols to convey those priorities from government to industry, and

• Determining how industry and government work together to protect those specific 'systems and assets' under fire, during an attack in both the orange and red scenarios outlined in the ICT Mobilization report."[46]

Any effective effort along those lines will require a major DoD role as the department has high-level capabilities that other government agencies/departments lack. For example, while the cyber security capabilities of the DHS have improved over time, it is perhaps clear enough, in light of various attacks on US government agencies such as the intrusion into the Office of Personnel Management,[47] that DHS does not yet have either the authority or the capability to respond to high-end cyberattacks. By way of illustration, an analysis by the General Accountability Office (GAO) found the intrusion protection system utilized by the DHS has limited capability. Specifically, GAO stated that the DHS system "is not fully satisfying all intended system objectives," "has limited ability to detect intrusions within observed network traffic," and "is unable to detect exploits across all types of network traffic."[48]

A report by Senator Tom Coburn, based on the GAO analysis, further stated that there are limitations to DHS's current capacity to work effectively with critical infrastructure, noting:

> "[T]here are open questions about how

[46] Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I - Incident Response* (June 2016), 7, https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

[47] US Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," News Release, June 4, 2015, https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/. See also, Committee on Oversight and Government Reform, US House of Representatives, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," September 7, 2016, www.oversight.house.gov.

[48] General Accountability Office, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, (January 2016), 16, 17, http://www.gao.gov/assets/680/674829.pdf.

> effectively DHS and NPPD [National Protection and Programs Directorate] are managing their efforts to partner with critical infrastructure sectors, as was discussed earlier in the report evaluating DHS's counterterrorism mission and information sharing with the private sector owners and operators of critical infrastructure."[49]

The foregoing is not to suggest that the DoD ought to act alone. Coordination should be with both DHS and the Department of Energy (DOE).[50] DHS is strengthening its capabilities and, according to the Cybersecurity National Action Plan, will "increase[e] the number of federal civilian cyber defense teams to a total of 48."[51] While DHS provides important support through the work of the ICS-CERT,[52] including training for eliminating malware and remediating networks, there are response functions that DHS does not perform that may be necessary.[53] For example, ICS-CERT does not provide staff to utilities that would be able to access their systems to eliminate malware and provide remediation tools. To create such a capability at DHS would require substantial additional resources. However, the DoD National Mission Teams (NMTs) and the National Guard are already focused on such issues and could provide assistance, especially if appropriate planning were undertaken. In coordination with DHS and other ongoing efforts by the federal government, a capability to deal with high-end attacks must be developed that incorporates and includes the advanced capabilities and expertise of DoD.[54] To that end, the Department of Defense has a key role, in coordination with the civil authorities and the ISPs and grid operators, in protecting and generating resilience for key critical infrastructure. While the DHS and the DoD have signed a memorandum of understanding (MOU) to facilitate their working together, the MOU does not focus on high-end attack and needs to be revised.[55] Likewise, while DoD personnel are present in certain of the departmental operational centers,[56] that involvement is not directed at the issues presented by high-end attacks.

Similarly, while the recently enacted Fixing America's Surface Transportation Act (FAST Act) authorizes the secretary of energy to order emergency measures if the president finds a grid security emergency,[57] there remains a lack of planning and development of capabilities to implement the act. To be sure, the act has useful provisions. In an emergency, the secretary of energy can issue any order he or she deems necessary to protect or restore the reliability

[49] Senator Tom Coburn, *A Review of the Department of Homeland Security's Missions and Performance* (January 2015), 92, https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE.

[50] "Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. . . . Synchronization among DHS, DOJ, and DOD not only ensures that whole of government capabilities are brought to bear against cyber threats, but also improves government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector." Deputy Secretary Jane Hall Lute, US Department of Homeland Security, Before the House Committee on Homeland Security (March 13, 2013), http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-LuteJ-20130313.pdf.

[51] The White House, Office of the Press Secretary, "Press Release: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[52] The ICS-CERT is the DHS's Industrial Control System Computer Emergency Readiness Team. See "The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)," ICS-CERT, https://ics-cert.us-cert.gov/.

[53] ICS-CERT focuses on analysis and information sharing. See Paul Stockton, *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*, Johns Hopkins Applied Physics Laboratory (2016), 25, http://www.jhuapl.edu/ourwork/nsa/papers/PostCyberAttack.pdf: "Specific support missions include the following: Responding to and analyzing control systems related incidents; Analyzing vulnerabilities and malware; Developing situational awareness in the form of actionable intelligence; Coordinating the responsible disclosure of vulnerabilities/mitigations; Sharing and coordinating vulnerability information and threat analysis through informational products and alerts."

[54] One example of a potentially very useful program being developed by DARPA that could vastly improve the electric grid operators' and ISPs' ability to understand and counter cyber threats is a program called Rapid Attack Detection, Isolation and Characterization Systems (RADICS). This DoD initiative advances the development of forensic tools that will require less delay or disruption of system restoration operations. RADICS can also provide extremely valuable situational awareness to utility operators by providing them with information about power outage locations. For a cyberattack where adversaries can spoof attacks, the RADICS initiative includes an effort to provide technologies for situational awareness that would be resistant to such spoofing risks. Statement by Arati Prabhakar, Director, DARPA, Before the Subcommittee on Emerging Threats and Capabilities Armed Services Committee, US Senate, April 12, 2016, 10-11, http://www.armed-services.senate.gov/imo/media/doc/Prabhakar_04-12-16.pdf.

[55] US Department of Defense, *DoD Cyber Strategy*, 5; "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," September 2010, https://www.dhs.gov/sites/default/files/publications/20101013-dod-dhs-cyber-moa.pdf.

[56] See Eric Chabrow, "DHS, DoD to Tackle Jointly Cyber Defense: NSA Cytological Know-How Will Aid DHS to Combat Cyber Threats," GovInfoSecurity, October 14, 2010, http://www.govinfosecurity.com/dhs-dod-to-tackle-jointly-cyber-defense-a-3010.

[57] Grid security emergency is defined to include "a malicious act using electronic communications or an electromagnetic pulse, or a geomagnetic storm event." See FAST Act, Section 215A (a)(7)(A)(i).

of critical electric infrastructure or of defense critical electric infrastructure, calling on utilities, NERC, and regional entities to implement emergency security measures. Additionally, the secretary and "other appropriate Federal agencies" shall provide temporary access to classified information about the grid security emergency to entities that are subject to an order for emergency measures. However, the act does not mention anything about the type of security measures DoE can direct and whether such measures would include involvement of DoD.[58]

III. DOD'S ROLE IN SUPPORT OF CIVIL AUTHORITIES

The 2015 *DoD Cyber Strategy* provides the foundation for a DoD role in a cyberattack against the US power grid and ISPs, but it does not provide explicit direction as to how DoD would help grid operators or ISPs operators in conducting such operations. Rather, the strategy provides a framework to develop the plans for possible DoD support while leaving key issues unresolved.

It is imperative to tackle these unresolved issues related to DoD's possible roles. A first step is to recognize that such activity by the DoD is fully in keeping with the long-standing Department of Defense function to provide support to civil authorities when civil capabilities are inadequate to meet critical challenges. This is equally relevant to cybersecurity issues as the MOU between DHS and DoD implies, and the National Cyber Incident Response Plan does state that DoD "may" be engaged if DHS requests.[59] It is therefore useful to review the organization and procedures of so-called Defense Support to Civil Authorities (DSCA) to understand the context of the steps necessary to make DoD roles effective in the context of a high-end cyberattack.[60] A recent report by the GAO provides a description:

> "When authorized to provide support to civil authorities for domestic emergencies, DOD may provide capabilities and resources—such as military forces (including the National Guard under Title 10 and Title 32, U.S. Code), DOD civilians, and DOD contractors. DOD components can also provide support to civil authorities under separate authority. For example, the DOD Cyber Crime Center can support digital and multimedia forensic requests and provide training services to non-DOD government organizations. Additionally, the National Security Agency, as an element of the Intelligence Community, is authorized to provide any other assistance and cooperation to law enforcement and other civil authorities not precluded by applicable law."[61]

The DSCA effort engages all elements of the DoD:

> "In an effort to facilitate DSCA across the nation and at all organizational levels, DOD has assigned responsibilities . . . DOD's Assistant Secretary of Defense for Homeland Defense and Global Security is the principal civilian advisor responsible for homeland defense, DSCA, and cyber policy for the department . . . The Chairman of the Joint Chiefs of Staff advises the Secretary of Defense on the effects of requests for DSCA on national security and identifies available resources . . . U.S. Northern Command and U.S. Pacific Command provide support to civil authorities . . . U.S. Cyber Command synchronizes the planning for cyberspace operations . . . The National Guard Bureau . . . coordinate[s] communications between DOD components and states for National Guard matters and conducts an annual assessment on the readiness of the National Guard to conduct DSCA activities."[62]

While DSCA is therefore generally well-established and applies to cybersecurity, the discussion below focuses on critical additional essential steps for dealing with high-end cyberattacks. The discussion sets forth how to develop contingency planning with civil authorities and the ISPs and electric grid operators, and how to undertake the necessary steps to make such planning effective in the event of a high-end attack.

[58] The law also directs the Federal Energy Regulatory Commission (FERC) to provide a mechanism for cost recovery if costs for compliance with an order cannot otherwise be recovered. See FAST Act, Section 215A, https://www.gpo.gov/fdsys/pkg/PLAW-114publ94/pdf/PLAW-114publ94.pdf.

[59] US Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 30, 2016, 7, https://www.us-cert.gov/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf.

[60] The *DoD Cyber Strategy* calls for DoD to "develop a framework and exercise its Defense Support of Civil Authorities (DSCA) capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector in an emergency if directed." US Department of Defense, *DoD Cyber Strategy*, 22.

[61] General Accountability Office, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents* (April 2016), 6-7.

[62] Ibid., 7-8.

IV. CRITICAL STEPS

In a high-end conflict, the military will rely heavily on the availability of the telecommunication and electric grid networks, and those networks likewise will likely need the assistance of the military to remain operationally effective, especially as an adversary in a high-end conflict can be expected to attack on a repeated basis. Understanding cross-sectoral dependencies and potential cascading effects from attacks will be crucial. Accordingly, for mission assurance and to achieve deterrence and/or successful defense with respect to such a conflict or potential conflict situation, particularly against high-end cyber adversaries, the military, civil authorities, and the ISPs and grid operators will need to work closely together both prior to and during the conflict. This will be true both in the United States and in the forward theaters where conflict is likely to occur. Accomplishing the necessary effective planning and operations will involve two overlapping sets of requirements:

- The military needs to develop a concept of operations that allows it to determine the required support from the ISPs and the electric grid in a high-end contingency (such as defense of the Baltics) and to provide the basis for a prioritized approach to cyber protection, resilience, and recovery of those networks. To prioritize mission-essential networks and industrial control systems that are critical for responding to regional crises, coordination with civil authorities and the ISPs and electric grid operators both prior to and during a crisis will be necessary.
- The civil authorities and the ISPs and electric grid operators need to develop contingency planning to elucidate what support from the military is required to provide the protection, resilience, and recovery necessary to maintain adequate telecommunications and grid operations for the nation in the event of a high-end contingency. The grid and ISP operators have unique knowledge of their specific system architectures and restoration plans and are the best experts to convey that information to the military so the military is ready to actively support their efforts both during an attack and for post-cyberattack restoration. Without this foreknowledge about the specific systems, DoD personnel who undertake to assist during a crisis would be unable to be effective and could in fact cause harm to the systems and contribute to other adverse consequences.

To accomplish these objectives, six actions need to be undertaken:

First, contingency plans for military, civil authorities, and ISP and electric grid operator interactions must be established for a high-end contingency through the use of an effective planning process supported by regular exercises and detailed playbooks that are routine in other emergency scenarios such as storms, fires, and earthquakes.

- As the NSTAC's and Homeland Security Advisory Council's analyses show, the requisite planning is not now in place. PPD-41 is a sensible action, but does not include any reference to the DoD and does not create mechanisms for dealing with a high-end attack, although the *DoD Cyber Strategy* plainly contemplates action by the DoD in conjunction with such attacks. DoD's efforts under other types of DSCA provide a model to help create the necessary planning, but it will be crucial to have a much more developed process with civil authorities and the ISPs and grid operators to achieve the necessary objectives. The planning process is yet to be developed; it will need to coordinate with actions taken for lower-level threats, but it will need to be more robust. Some important questions to be determined include the following:
- The objective of contingency plans need to be developed. Prioritization is required and that will require focus on particular infrastructures and particular companies.[63] An attempt to deal with everything equally will fail for lack of resources. Prioritization will need to take into account such factors as the importance of balancing authorities, the fact that the top ten largest electric generator companies have about 40 percent of US generating capacity, and the importance of cross-sector

[63] The Homeland Security Advisory Council underscored the importance of prioritization: "Prioritize which infrastructure is of the greatest risk to cyber-attack. Government, in consultation with the private sector, should determine priorities in terms of critical infrastructure at greatest risk so that response, recovery, and restoration priorities are clearly understand [*sic*] in the immediate aftermath of an incident. To the extent possible, this pre-identification would lead to increased attention to 'left-of-boom' activities, including relationship building between appropriate stakeholders. This process should include identifying specific systems and assets that may be at risk (using classic risk formulation of Risk = Threat x Consequence x Vulnerability) as opposed to simply identifying companies." Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I - Incident Response* (June 2016), 29, https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

During the Cyber Shield 2016 training exercise at Camp Atterbury, Indiana, Army and Air National Guardsmen played as the blue team defenders. The exercise on April 20, 2016, is designed to develop and train forces to be cyber-capable. Ongoing exercises led by DoD need to be developed and lessons learned implemented into a combined contingency plan. *Photo credit:* United States Army.

interdependencies such as the electric grid to telecoms and finance.

- Pre-attack plans ought to include a mechanism for cross-sector coordination between the DoD, civil authorities, and the ISPs and grid operators.[64] With the possibility of simultaneous attacks against multiple sectors with multi-regional or nationwide effect, a swift response by the United States will be important. Only with such response and recovery plans in place prior to an attack will a rapid response be possible.[65] Such actions should be taken in coordination with DoD, the civil authorities, ISPs, and grid operators.

- While there are ongoing exercises led by DoD, in particular through Cyber Guard, Cyber Shield, and Vista Host II, these efforts need to be further developed and lessons learned need to be implemented into a combined contingency plan approach with the civil authorities, ISPs, and major electric grid operators. Techniques, tactics, and procedures work best when established and tested in advance and not when they are created on the fly in the context of a conflict. Moreover, while exercises like GridEx III have highlighted the cascading failures that would be created by an attack on the power grid and the ways that resulting disruptions in the communications sector would create power restoration challenges,[66] more joint exercises involving multiple critical infrastructure sectors are needed to identify the multiple interdependences between the different sectors and test the operational effectiveness of response and restoration actions across multiple sectors.[67]

Second, clear chains of command for a high-end contingency must be established between the civil

[64] According to DHS, "No such mechanism [across the sectors] for large-scale operational coordination exists today." Ibid., 13.

[65] According to the NERC's study on severe impact resilience in 2012, in the event of a significant cyberattack, it is likely that complete restoration of electric service may not be possible for many weeks or even months. See, NERC, Sever Impact Resilience Task Force, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, 10, http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

[66] GridEx is a biennial grid exercise designed to exercise utilities' crisis response and recovery procedures, improve information sharing during a crisis, and engage senior leadership. The last one, GridEx III, was held in November 2015, http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx. In April 2016, DoE led the Clear Path IV in Portland, Oregon, and Washington, DC. See Hoffman's written statement for testimony on April 14, 2016.

[67] One recommendation in the Homeland Security Advisory Council report was to create a "cross-sector emergency response team." Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 30.

authorities and the DoD and within the DoD itself, in addition to an operational mechanism that includes the ISPs and the electric grid operators, to allow prompt and responsive actions.

- For most contingencies, the usual DoD role of support to civil authorities will apply. However, in the event of a high-end attack, DoD will likely need to take the lead role. Establishing and exercising the procedures necessary to accomplish this before a significant crisis arises will be critical. The DoD-DHS MOU should be revised to provide for such a contingency.

- Additionally, the DoD needs to clarify its internal chain of command. In its report assessing DoD's support to civil authorities, the GAO found that DoD's DSCA "guidance does not clearly define its roles and responsibilities for cyber incidents," and "guidance documents are inconsistent on which combatant command would be designated the supported command and have primary responsibility for supporting civil authorities during a cyber incident. U.S. Northern Command's DSCA response concept plan states that U.S. Northern Command would be the supported command for a DSCA mission that may include cyber domain incidents and activities. However, other guidance directs and DOD officials stated that a different command, U.S. Cyber Command, would be responsible for supporting civil authorities in a cyber incident."[68]

. . . [C]lear chains of command for a high-end contingency must be established between the civil authorities and the DoD and within the DoD itself. . .

There are multiple ways to establish the command chain. The key is to do so, and to eliminate ambiguity.

In addition, the establishment of a planning and operational mechanism to include civil authorities, DoD, ISPs, and grid operators is necessary. PPD-41 created a "Cyber Unified Coordination Group" (Cyber UCG), but, as noted above, it does not include the DoD. Moreover, it is to be created only when an incident occurs and is designed to create "unity of effort," not to alter agency responsibilities. While this is an understandable approach for cyber incidents not involving a conflict, it will not be effective in the context of conflict. The Cyber UCG as established is too bureaucratically cumbersome and lacks the requisite DoD involvement to be effective in such a crisis. Conflict requires clear chain of command. Accordingly, a more effective approach must be created. One option would be to establish a national Cyber Conflict Coordination Board ("the Board") to oversee and implement operational interaction between DoD, the civil authorities, ISPs, and grid operators with flexible membership to enhance the defense and resilience of the ISPs and electric grid operators.[69] The Board would build on the Cyber UCG framework, but would also provide for actual command relationships in lieu of the much slower and likely more ineffective coordination set out in PPD-41. Furthermore, Congress should consider creating a requirement for unified cyber actions along the lines of the Goldwater-Nichols Act, which realigned the workings of the Department of Defense and required joint actions among the four services for war-fighting purposes. Such legislation could include the establishment of the Board as the mechanism to help achieve coordinated joint operations.

Third, certain actions taken in advance of an attack will be required to establish effective protection and resilience. Numerous analyses have demonstrated that effective cyber defense and resilience cannot wait for an actual attack. For example, the NSTAC report on "Big Data Analytics" stated:

> "It is possible to thwart an entire adversary group campaign by deploying the correct prevention control at the precise spot in the attack lifecycle. Moreover, deploying as many prevention controls as possible, at every stage in the attack lifecycle, almost assuredly guarantees that the specific adversary campaign will not succeed."[70]

[68] Government Accountability Office, *Defense Civil Support: DOD Needs to Clarify Its Defense Support of Civil Authorities during Cyber Incidents,* April 2016, summary page, http://www.gao.gov/assets/680/676322.pdf.

[69] National Security Telecommunications Advisory Committee, *Report to the President*, 31; see Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 15 (*"To pilot the development of a near-term capability for operational coordination, the electric, financial, and communications sectors could explore options for an interim coordinating body."*

[70] *NSTAC Report to the President on Big Data Analytics*, (May 2016), 28 [hereinafter *NSTAC Report on Big Data*], https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Big%20Data%20

DARPA has established a program "detailing research aims for the early detection of cyber-attacks to power-grid infrastructure and seeking ways to reduce the time required to restore power."[71] An important concept that both the NSTAC report and the DARPA project build on is that of the cyber "kill chain," which recognizes that there are multiple stages in a cyberattack prior to the actual activation of malicious code:[72]

> "Cyber attackers target systems not in single incidents and breaches but, instead, through a campaign of efforts that enables access and provides sufficient information to devise an effect . . . The multiple stages, or exaggerated kill chain, provide additional opportunities for defenders to increase the adversary's cost of an attack and to position themselves to detect and disrupt attackers before they reach their goal."[73]

As the foregoing suggests, prior to conflict, intrusions need to be blocked as much as possible; malware needs to be removed; and capabilities for maintaining data integrity, confidentiality, and availability need to be built and exercised. What is critical to this effort is the use of a variety of adaptive resilience techniques, ranging from diversity and redundancy to moving target defenses and deception.[74] All these resiliency features require development and implementation prior to conflict. Not all attacks can be detected, though there is great value if that can be accomplished, but their effects can be mitigated if steps are taken in advance.[75]

DoD can utilize the knowledge generated in defending its own networks to assist other defenders, and undertake research and development through DARPA and other DoD-applied research and development activities to provide advanced capabilities. For critical networks, utilizing highest-level standards even beyond what the companies would undertake on their own would have value for national security reasons. For example, one approach would be to uniformly enforce standards for network traffic, including control of malformed packets, and use capabilities such as the Domain Name System Security Extensions (DNSSEC) and Border Gateway Protocol Security (BGPSEC), to increase wide band network resiliency.[76] The Federal Communications Commission has the authority to require ISPs to take such actions, but the potential benefits and costs of such efforts should be evaluated in connection with the coordinated approach to high-level conflict discussed herein.[77] Furthermore, the government ought to review whether the private sector will need financial assistance carrying out such operational defensive actions and determining how such assistance could be provided.

Fourth, the role of the NMTs (being established by Cyber Command to respond to cyberattacks of significant consequence) and the National Guard must be developed and clarified.[78] A determination

Analytics%20%285-11-16%29-%20508%20compliant.pdf.

[71] DARPA, DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack (December 2015), at http://www.darpa.mil/news-events/2015-12-14.

[72] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin (2014), www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.

[73] Michael J. Assante and Robert M. Lee, *The Industrial Control System Cyber Kill Chain* (Bethesda, MD: SANS Institute, October 2015), 1, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

[74] See Harriet Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," (2010), https://www.mitre.org/sites/default/files/pdf/10_3301.pdf. One analysis has proposed: "These measures include (1) hardening their primary control centers against attack; (2) building robust backup control centers; (3) securing their gold copies of operational technology (OT) system software and exercising to rapidly install it if needed; (4) developing 'spare-tire' control mechanisms that will not provide the full functionality of regular systems but can sustain limited vital operations; and (5) maintaining fallback mechanical controls that would otherwise be at risk of degrading and becoming inoperable." Stockton, *Superstorm Sandy*, 17.

[75] *NSTAC Report on Big Data* stated on page 29, "The ability to detect the event, and determine what type of event is occurring is key to an effective response. Through the use of BDA [Big Data Analysis] at the detect stage, the response can be more effective and reduce the consequences that might require recovery. Together, the use of BDA to enhance detection and response is key to minimizing the impact of a cyber event."

[76] Melissa Hathaway and John Savage, "Stewardship of Cyberspace: Duties for Internet Service Providers," in *Cyber Dialogue 2012* (March 2012), http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.

[77] It should also be possible to rapidly move to automated methods for sharing threat and response information within and across critical infrastructure service providers. For example, STIX (Structured Threat Information eXpression), TAXI (Trusted Automated eXchange of Indicator Information), and CYBOX (Cyber Observable eXpression) could be uniformly adopted as standards and enforced across sector-specific oversight authorities for both private and public sectors. See "Information Sharing Specifications for Cybersecurity," US-CERT, United States Computer Emergency Readiness Team, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

[78] A number of states are establishing plans for their state National Guard organizations to create cyber protection teams that would be activated to help respond to requests for assistance after a cyber incident. See State of Michigan Executive Office, *Michigan Cyber Disruption Response Strategy* (Lansing, MI: State of Michigan Executive Office, September 16, 2013), https://www.michigan.gov/documents/

should be made whether those capabilities should be complemented by private sector entities who would work under government direction and control in connection with high-end contingencies.

- Currently there are thirteen NMTs being established by Cyber Command to focus on cyberattacks of significant consequence. The National Guard is likewise increasingly focused on cyber, including with respect to critical infrastructure, and is increasing the number of cyber protection teams[79] with plans for thirty Army National Guard cyber units and seventeen Air Force National Guard units by 2019,[80] including training cyber teams in the protection of industrial control systems. One such team is Washington State's 262nd Network Warfare Squadron.[81] Other states are taking similar steps.[82] This is a combined total of sixty cyber units focused on non-DoD systems as compared to sixty-eight teams to defend DoD's own networks. Given there are approximately thirty-two hundred electric grid operators in the United States, it seems unlikely that even sixty teams could accomplish across-the-board protection, resilience, and recovery in the event of a high-end attack. If, however, the contingency plans recommended above were developed, that would allow for prioritization of the sixty teams as well as for coordination with the DHS civilian cyber defense teams.

- It will be important to define the roles of the NMTs and the National Guard both before and during a conflict. One useful effort being undertaken by the National Guard is the development of assessments, working with existing state authorities. Given the National Guard is not subject to active duty limitations when under state control, they could be utilized to go beyond assessments and assist with monitoring, for example, of key electric grid operators. This would need to be done in coordination with the companies. NMTs and the National Guard will not have the degree of expertise that ISPs and grid operators have in their respective domains, but a combined effort utilizing exercises and modeling can establish tactics, techniques, and procedures for operating in a degraded environment.

- Even with NMT and National Guard capabilities there may not be enough capacity to respond effectively to a high-end attack. This raises the issue of whether and to what extent private sector entities should have a role. As one analysis stated:

> "However, the same risk of multiple nationwide cyber attacks that complicates mutual assistance agreements could also create problems when relying on contractors. Individual companies may be called on to serve multiple clients at the same time (in both the public and the private sectors), requiring staffing levels far beyond those necessary for the typical levels of support. Contractor surge capabilities will be essential to meet such demands; otherwise, utilities will be left without the assistance they need."[83]

Adding certified defenders to support DoD and infrastructure provider capabilities would enhance the capacity to act in advance. For example, with the agreement of the grid providers (by contract or otherwise), certified active defenders could operate inside their networks and enhance protection and resilience.[84] In such instances, the certified active defenders could assist the sectors by rapidly identifying the threat, characterizing the malware used in the attack, eradicating the malware from the networks, and assisting in assessing the damage during a cyber event. Of course, as with NMTs and the National Guard, such defenders would need prior interaction and exercises with ISPs and grid operators

cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf. While this is an important step for progress, more needs to be done to make such a system effective. However, at the federal level, there is currently no established plan for how governors will be brought into the response coordination process after an incident. To ensure unity of effort between the federal agencies and the states this needs to occur. For example, DHS's 2011 Interim National Cyber Incident Response Plan did not indicate how governors would partner with federal agencies and private sector representatives to coordinate cyber response efforts within their states. See US Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version*, September 2010, http://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf.

[79] National Guard Association of the United States, Guard Names Sites of Cyber Units (December 2015), http://www.ngaus.org/newsroom/news/guard-names-sites-cyber-units.

[80] Scott Maucione, "As Cyber Units Expand, National Guard Has Training Backlog," March 16, 2016, http://federalnewsradio.com/defense/2016/03/cyber-units-expand-national-guard-training-backlog/.

[81] 24th Air Force Public Affairs, "24th Air Force Commander Visits Washington ANG units," May 22, 2014, http://www.24af.af.mil/News/Article-Display/Article/731780/24th-air-force-commander-visits-washington-ang-units.

[82] Stockton, *Superstorm Sandy*, 34.

[83] Ibid., 13.

[84] See Franklin D. Kramer and Melanie J. Teplinsky, *Cybersecurity and Tailored Deterrence* (Washington, DC: Atlantic Council, December 2013), http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf.

to be effective. Accordingly, a valuable step to enhance deterrence and defense would be for legislation to be enacted that enables the government to authorize "certified active defenders" to work with USG prior to and in times of conflict for defense and offense as determined by USG.

Fifth, DoD should establish programs and funding to support resilience and recovery.

- The USG should leverage the Defense Production Act to ensure that readiness reserves in hardware and systems exist for critical infrastructure providers as they reconstitute/recover.[85] The DoD and the USG have provided funding to key industries in the past as part of national security efforts. Those programs include the Civil Reserve Air Fleet and those that maintain American ocean shipping.[86]

The DoD could provide a contractual program for the purchase of key infrastructure components for the ISPs and the electric grid operators. Companies who participate could be further incentivized through payments and limited liability protection to provide greater levels of security to their industry supply chain and vendor management processes and to adopt best-practice secure engineering and better engineered products.[87]

DoD funding could also support DOE efforts contemplated under the Strategic Transformer Reserve of the FAST Act. Given that large power transformers require long manufacturing lead times and cannot be easily replaced or transported in the event of damage or disruption, a reserve is intended to increase the availability of spare transformers and emergency mobile substations that are staged at pre-designated locations for timely delivery in the aftermath of an energy grid disruption. Under the act, DOE, in consultation with Federal Energy Regulatory Commission and NERC, must develop a plan for a reserve. The FAST Act does not provide DOE with any new authority to create a reserve, and it is not clear whether further congressional action would be required. Furthermore, DOE's plan to Congress will need to include funding options.[88] A joint DoD-DOE program could support the reserve.[89]

Sixth, offense will be a key element of effective operations. Prior to conflict, the United States should lead an expanded "fusion" effort, largely led by civil authorities, to bring to bear intelligence, cyber, financial, law enforcement, and other capabilities to disrupt the actions of state and state-associated entities undertaking adversarial cyber-action. The model would build off the fusion teams utilized in counter-terror activities, and leverage previous law enforcement–led activities that have resulted in the disruption of criminal cyber-networks and enablers like botnets. Importantly, these efforts would focus on developing and implementing sustained campaigns for countering adversarial cyber-action, and include the participation of allies and other partners. The USG should develop a greater array of campaigns to legally

[85] The act authorizes the president to "require persons (including businesses and corporations) to prioritize and accept contracts for materials and services as necessary to promote the national defense." Jared T. Brown and Daniel H. Else, "The Defense Production Act of 1950: History, Authorities and Reauthorization," Congressional Research Service, June 28, 2014, summary page, https://www.fas.org/sgp/crs/natsec/R43118.pdf; See also Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," Chap. 6 in Burns and Price (eds.), *Securing Cyberspace.*

[86] In the Civil Reserve Air Fleet (CRAF) program: "Selected aircraft from U.S. airlines, contractually committed to CRAF, augment Department of Defense airlift requirements in emergencies when the need for airlift exceeds the capability of military aircraft. . . . To provide incentives for civil carriers to commit aircraft to the CRAF program and to assure the United States of adequate airlift reserves, the government makes peacetime DOD airlift business available to civilian airlines that offer aircraft to the CRAF. DOD offers business through the CRAF Charter Airlift Services contract." See "Civil Reserve Air Fleet," US Air Force, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104583/civil-reserve-air-fleet.aspx. Similarly, "The NDAA of 2013 requires that the Secretary of Transportation, in consultation with the Secretary of Defense, to establish a fleet of active, commercially viable, militarily useful, privately-owned vessels to meet national defense and other security requirements." See "Maritime Security Program," Maritime Administration, August 2016, https://www.marad.dot.gov/ships-and-shipping/strategic-sealift/maritime-security-program-msp/.

[87] The CRAF program, in fact, provides for DoD inspection to ensure that appropriate engineering and maintenance standards are met.

[88] Beyond DOE, there are industry initiatives focused on improving access to necessary equipment during a time of greater need. Such industry equipment-sharing programs like Grid Assurance, the Spare Transformer Equipment Program (STEP), Wattstock, and SpareConnect, which were established to mitigate the risk of physical damage caused by natural hazards or kinetic attacks to equipment, could serve as a model for industry sharing when equipment is damaged or destroyed because of a cyberattack. In addition, Edison Electric Institute is working with Class 1 Railroads to plan for possible events that would require the movement of transformers. Such industry initiatives ought to be encouraged.

[89] The FAST Act states that FERC will establish a mechanism for recovery of "substantial costs" to comply with emergency orders, but there is still uncertainty about recovery costs. For example, with respect to emergency orders related to defense critical electric infrastructure, the provision of the act explicitly requires the owners and operators of such infrastructure to "bear the full incremental costs of the measures." It does not mention that such funding may not be available. Also, for those entities not subject to FERC's rate jurisdiction, such as public power entities or electric cooperatives, there is no mention of cost recovery for them. A DoD-funded approach to cover such national security costs would be highly worthwhile.

Left: Marines with 1 Marine Expeditionary Force and sailors with 553 Cyber Protection Team. *Photo credit*: Cpl Garrett White. Right: A Slovenia delegation member at the Exercise Combined Endeavor 2013 at Grafenwoehr, Germany on September 13, 2013. Forty NATO, Partnership for Peace, and coalition partner nations convened for the largest command, control, communications, and computer (C4) exercise in the world. Source: United States European Command.

and/or technically disrupt attributed adversaries' activities against USG-declared critical infrastructure owned and operated by the private sector. Simply by way of example, the DoD has a monitoring capability outside the networks of the ISPs and grid operators, and this would allow for a combined effort with such providers (including effective interaction between the telecoms and the electric grid operators).

Campaign planning should include courses of action to respond to so-called hybrid warfare, including actions directed at the United States and its allies. In other arenas, the United States has developed "flexible deterrent options," and such capabilities should be created in cyber so that commanders will have a full spectrum of options to utilize if the president determines it appropriate.

Additionally, cyber offensive capabilities will be an important part of resilience. Locating and degrading adversary offensive cyber capabilities will be valuable, especially to limit multiple attacks. Combining intelligence and offensive capabilities will provide the basis for disrupting adversary cyber command and control to, for example, limit DDOS attacks. In the event of conflict, cyber capabilities can also target military capabilities such as sensors, communications, logistics, and military-supporting infrastructures. In a similar fashion to air campaign planning, prior analysis of targets, including the probability of collateral consequences, could be undertaken, enabling the development of cyber-attack "campaign packages" for commanders. Providing such capabilities to a defending force would have significant military value. Accordingly, cyber offense needs to be integrated into US, allied, and partner military strategy to enhance overall deterrence.

V. CYBER, EXTENDED DETERRENCE, AND FORWARD THEATERS

In a conflict, cyber security will be as or more important in forward theaters as it will be in the United States. Most US allies and partners do not have the same cyber capabilities as DoD, yet it will be their infrastructures and national capabilities that US forces will be relying upon for numerous tasks. Accordingly, the concept of "extended cyber deterrence" will be an important role for the DoD in connection with each of the theaters noted above. The concepts are set forth in the issue brief "Cyber, Extended Deterrence, and

NATO,"[90] but their application goes beyond NATO to all arenas where US critical interests are intertwined with allies and partners.

Most obviously, the United States will continue to develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of US war-fighting capabilities. As noted above, cyber tools potentially could disrupt an adversary's communications, logistics, sensors, and military-supporting infrastructure. The secretary of defense has stated that cyber is currently being used in the conflict with ISIS,[91] and NATO has recently designated cyber an operational domain.[92] Cyber will continue to be integrated into combat planning.

Cyber security will be important not only for US forward forces, but also for the militaries and the critical infrastructures of host nations. It is notable that in each of the theaters that the United States plans for, the potential adversary has been identified as the source of significant cyber intrusions. Russia is responsible for the hacking of the Democratic National Committee, among many other cyber incidents.[93] China is responsible for the attack on the Office of Personnel Management and Chinese officers have been indicted for continued cyber espionage.[94] Iran is behind the attack on Saudi Arabia's oil company and Iranian hackers have been indicted for attacks on American banks.[95] North Korea is behind the attack on Sony and has regularly attacked South Korean networks.[96] What these attacks demonstrate is the vulnerability of host nations to cyberattack, a vulnerability that could significantly undercut deterrence or the capacity of the United States and its allies and partners to prevail in a conflict. To mitigate such vulnerability, three key elements should be used:

> . . . [T]he United States needs to act as a "cyber framework nation" to support host nation capabilities. . . . to enhance protection, resilience, and restoration.

First, the United States needs to act as a "cyber framework nation" to support host nation capabilities. This would involve the establishment, transfer, training, and support of cyber capabilities to enhance protection, resilience, and restoration. For example, the United States could help a less cyber-capable ally establish an effective intrusion protection system, provide forensic support, and develop resilience capabilities to be utilized in the event of an attack by an adversary.

There are several ways to undertake such efforts but one of the most useful would be to utilize the National Guard's State Partnership Program. The program pairs state National Guard units with seventy-six countries.[97] As noted above, the National Guard is substantially increasing its cyber capabilities, including its focus on critical infrastructures. That expertise can be utilized in working with allies and partners in conjunction with the relevant combatant command. The National Guard's partnership efforts can build on what the NMTs and the National Guard are doing in the United States, adapted, of course, to the particulars of the host nation. The National

[90] Kramer et al., "Cyber, Extended Deterrence, and NATO." Portions of this section are taken directly from that article.

[91] US Department of Defense, "New Transcript, Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room," February 29, 2016, http://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the.

[92] Colin Clark, "NATO Declares Cyber a Domain; NATO SecGen Waves Off Trump," *Breaking Defense*, June 14, 2016, http://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/.

[93] David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked the D.N.C.," *New York Times*, July 26, 2016, http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0.

[94] Ellen Nakashima, "Chinese Government Has Arrested Hackers It Says Breached OPM Database," *Washington Post*, December 2, 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html; For the DoJ indictment of the Chinese hackers, see "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," Department of Justice Press Release, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[95] Ellen Nakashima and Matt Zapotosky, "U.S. Charges Iran-linked Hackers with Targeting Banks, N.Y. Dam," *Washington Post*, March 2016, https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html.

[96] Jack Kim, "North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul," Reuters, June 13, 2016, http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.

[97] Statement by General Frank J. Grass, Chief, National Guard Bureau, Before the Senate Appropriations Committee, Subcommittee On Defense (March 16, 2016), http://www.appropriations.senate.gov/imo/media/doc/031616%20-%20General%20Grass%20-%20CNGB%20-%20Testimony1.pdf.

Guard could also be part of an initiative to provide "fly away" cyber-warfare teams to provide host nation states' "blue team" assistance to "operate in degraded environments," including providing malware forensics and recovery/restoration support.

In addition to the National Guard, the DoD Cyber Crime Center (DC3) could have a valuable international role. DC3's current mission revolves around five focus areas: digital forensics, cyber training, technical solutions, Defense Industrial Base (DIB) cybersecurity, and analytics.[98] Like the Guard, DC3 provides tremendous depth and breadth of support; applied to international requirements it could enhance a greater USG role through a modest budget. DC3's mission could be expanded to support extended cyber deterrence, especially in the areas of building greater allied cyber resilience. Key elements could include growing international training and information-sharing programs for allies (similar to ongoing programs with DIB companies in the United States).

Second, associated with US assistance, it will be important for the host nation to establish operational partnerships with key private entities, including ISPs and power grid operators. As discussed in the context of the United States, military, telecommunications, and electrical grid operators should help create, in advance, capabilities that would mitigate a high-end attack. The United States, as a cyber framework nation, would help the host nation organize for this effort. Depending on the theater, it may be important to undertake such efforts on a regional, as opposed to a national, basis. Again, the United States will be well positioned to help create the necessary regional activities.

Third, host nations will need to undertake steps comparable to those identified for the United States. These include

- identifying highest-priority national military cyber assets and supporting telecom and power grid networks that would need to be protected;
- extending/enhancing automated intrusion protection and developing resilience efforts, starting with data classification and segmentation, to participating host nations' militaries, telecommunication companies, and electrical grids. It will be important to utilize high-end protection capabilities, such as multi-factor authentication, end-to-end data encryption, and diverse and redundant networks to ensure best information assurance practices in data confidentiality, integrity, and availability;
- increasing detection capabilities by provisioning shared cyber threat intelligence capabilities. A cyber threat intelligence capability would develop and share cyber indications and warnings regarding the movement of high-end state cyber-threat activity towards host nation networks and information assets; and
- developing cyber defense "playbooks" and training exercises for cyber-attack response, with techniques, tactics, and procedures (TTPs) developed to maximize the value of the defense and resilience capabilities noted above. National grid and telecommunications partners in the private sector would be included as part of the playbook TTPs and training exercises.

As previously discussed by the authors:

> "Initially, the cyber framework nation can help to establish or enhance an existing national framework. Over time, simulations, exercises, and information sharing will help direct and prioritize other efforts by exposing gaps and opportunities. Joint exercises, when effective, usually result in some degree of information sharing. Explicit and incidental information sharing, especially between private and public sector partners, will be a critical requirement if operational protection and/or resilience is to be achieved. Each country should pick a model it finds compatible, but the keys are a combination of speed and full interchange. In the US, one of the most effective models is the 'Information Sharing and Analysis Center (ISAC), a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.' ISACs are typically developed around a critical infrastructure sector, such as the electrical grid or telecommunications sectors. The Financial Services ISAC is often considered the greater among equals, as it has a highly automated system for rapid cyber threat information exchange."[99]

[98] See "DC3," DoD Cyber Crime Center, Air Force Office of Special Investigations, http://www.dc3.mil/index#capabilities.

[99] Kramer et al., "Cyber, Extended Deterrence, and NATO," 7. The internal quotation comes from Wikipedia, "Information Sharing and Analysis Center," https:// en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center.

As the foregoing indicates, cyber will be a critical element of high-end conflict. Enhancing deterrence and defense will require extensive actions by allied and host nation militaries along with civil authorities and the ISPs and grid operators in the host nation.

VI. CONCLUSION

High-end conflict will create challenging requirements for cyber, far beyond those that are already faced on an ongoing basis. The DoD needs to work with civil authorities and the ISPs and grid operators in the United States and forward theaters to create the prospects for deterrence and, if necessary, to defend and prevail in conflict.

Franklin D. Kramer is a distinguished fellow and on the board at the Atlantic Council and a former assistant secretary of defense.

Robert J. Butler is an adjunct fellow at the Center for a New American Security and served as the first US deputy assistant secretary of defense for cyber policy.

Catherine Lotrionte is the director of the CyberProject in the School of Foreign Service at Georgetown University, former counsel to the President's Foreign Intelligence Advisory Board, and former assistant general counsel at the Central Intelligence Agency.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org