Posturing U.S. Cyber Forces to Defend the Homeland

Colonel Jamel Neville

ABSTRACT

On March 21, 2022, the White House warned that Moscow is exploring options to attack US critical infrastructure in response to economic sanctions levied on Russia following its 2022 invasion of Ukraine. On May 25, 2023, the U.S. State Department issued a similar warning regarding Beijing's capabilities and intentions. As revisionist powers seek to disrupt the international order and cyber threats to critical infrastructure persist, the Department of Defense (DoD) must effectively position its cyber forces and capabilities to defend against cyber-attacks before they hit the homeland. An attack against the US power grid could result in multiple failures in life-sustaining infrastructure and significantly impact Joint Force power-projection capabilities. U.S. Northern Command (USNORTHCOM) must work closely with U.S. Cyber Command (USCYBERCOM) to orchestrate federal and non-federal stakeholders' cyber authorities, capabilities, and equities to posture DoD cyber forces to respond with speed and agility. However, the myriad of federal cyber laws, regulations, authorities, and public and private sector stakeholder equities could impede DoD's response efforts. National cybersecurity is "a team sport," but players tend to use different playbooks or play by different rules. Tools such as a DoD "Complex Catastrophe Cyber Stakeholders, Communications, Authorities, and Narratives" (C3 SCAN) framework could enable USNORTHCOM and USCYBERCOM to foster collaboration, validate plans and orders, enumerate and prioritize mission-relevant terrain in cyberspace, and ensure readiness for Defense Support to Cyber Incident Response (DSCIR).

Colonel Jamel Neville is the Marine Corps Cyberspace Warfare Group Commanding Officer. Previously, he served in various capacities throughout the U.S. Cyber Mission Force, including a joint force headquarters and joint task force director of operations (J3); cyber combat mission team and cyberwarfare task group commander; and deputy director for current operations (G33). Before becoming a cyberspace warfare officer in 2018, Col Neville served as a communications officer following his commissioning in 2000. He deployed to Operations ENDURING FREEDOM and FREEDOM'S SENTINEL and in response to defense support of civil authorities (DSCA). Col Neville also worked in the private sector as a defense consultant to The Joint Staff and Defense Threat Reduction Agency for several years. He has earned a Master's in strategic studies, a Master's in military studies, an MBA in information technology management, and a Bachelor's in fine arts. Col Neville is a certified information system security professional (CISSP).

POSTURING U.S. CYBER FORCES TO DEFEND THE HOMELAND

> When a cyber-attack can deliver the same damage or consequences as a kinetic attack, it requires national leadership and close coordination of our collective resources, capabilities and authorities.
>
> *– The President's National Infrastructure Advisory Council* [1]

Enemy attacks resulting in infrastructure damage are not new. As war raged throughout the European and Asia-Pacific regions, adversaries penetrated and maneuvered throughout key United States East Coast supply chain nodes starting in January, which eventually resulted in the deaths of thousands of people over the following several months. In February, adversarial attacks against one Southern California oil refinery generated mass hysteria across the West Coast. Adversaries operated undetected throughout the spring despite shared threat intelligence and lessons from the United States' allied partner in the weeks and months preceding the initial attacks. During the February attack, electricity and electromagnetic spectrum outages across Los Angeles and San Diego stemmed from the inability of the U.S. military and local authorities to coordinate responses, which exacerbated the already chaotic and confusing situation that day. Due to the war overseas, the military committed the preponderance of its focus and effort to operations abroad, resulting in an inability to surge forces to counter adversaries' asymmetric attacks against the homeland. While new federal authorities enabled innovative public and private sector partnerships and capabilities to thwart the malicious activities, the impact on the Northeast fuel *supply chain forced nationwide gasoline rationing throughout the next two years because of Germany's Operation Drumbeat, launched on January 14, 1942.*

INTRODUCTION

In the above vignette, German and Japanese submarine attacks against vulnerable targets along America's shorelines at the onset of World War II are an example of a complex catastrophe, which the federal government defines as:

> Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions.[2]

Operation Drumbeat illustrates how the U.S. was unprepared to counter the asymmetric attacks against merchant shipping across the East Coast by the Germans and the Santa Barbara Bankline Company aviation fuel storage farm by the Japanese, nor could it handle their non-kinetic effects.[3] The ominous potential for increased attacks threatened to plummet national oil supplies to intolerable levels, harming American and Allied war efforts and resulting in the death of thousands of seamen and civilians.[4] The grim outlook compelled greater unified action between the federal government, public, and private sector to detect and thwart the adversary.[5]

Though cyber-attacks on U.S. critical infrastructure may likely not produce the same devastating effects as German U-boats, America's fragmented and disorganized coastal defenses and delayed and unsynchronized military response actions in 1942 are worth some reflection.[6] Today, sophisticated cyber actors have the potential to exploit information and communication systems vulnerabilities to establish undetected access and control of these systems and produce detrimental effects.

As the Russo-Ukrainian war continues, Moscow increases its aggression against the West, U.S.-China tensions over Taiwan and other issues increase, and the U.S. faces the threat of sophisticated cyber-attacks against its critical infrastructure. On March 21, 2022, the White House warned that Moscow is exploring options to attack U.S. critical infrastructure in response to economic sanctions on Russia following its full-scale invasion of Ukraine. On May 25, 2023, the U.S. State Department warned that Beijing could launch cyber-attacks against oil and gas pipelines and rail systems after Microsoft analysts identified the campaign, dubbed Volt Typhoon, "could disrupt critical communications infrastructure between the United States and Asia region during future crises."[7]

While the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) collaborates with organizations to protect U.S. critical infrastructure, their efforts are more passive.[8] The Department of Defense (DoD) is ultimately responsible for posturing cyber forces for active defense against complex cyber-attacks by countering and blunting the offensive efforts of foreign adversaries. However, the myriad of federal cyber laws, regulations, and authorities; DoD inter- and intra-organizational relationships (e.g., interagency and intelligence community); and public and private stakeholder equities could hinder DoD's ability to prepare and respond with speed and agility in cyberspace.[9] National cybersecurity is "a team sport," as fittingly described by the U.S. Cyber Command (USCYBERCOM) Commander and Director of the National Security Agency (NSA), General Paul Nakasone.[10] Still, players on the same team may use different playbooks or play by different rules.

This article provides a methodology on how the DoD should team with CISA, the FBI, and other federal and non-federal stakeholders to counter, prevent, or minimize the impacts of large-scale cyber-attacks against US critical infrastructure networks. Russian aggression, geopolitical tensions, and future strategic threat assessments highlight the need for unified action in cyberspace. DoD – specifically, U.S. Northern Command (USNORTHCOM) and supporting cyber forces from USCYBERCOM – must understand the laws and policies that could affect (either hinder or enable) DoD cyber protection and offensive operations before, during, and after a complex cyber-attack against the homeland. While DoD cyber force and capability positioning are important planning factors, DoD's ability to effectively orchestrate stakeholders' cyber authorities, capabilities, and equities to protect against, prevent, mitigate, respond to, and recover from complex catastrophes of this scope and scale is paramount.[11]

Background

In 2018, the then-USNORTHCOM Commander, General Terrance O'Shaughnessy, proclaimed that the U.S. homeland is no longer a sanctuary.[12] He aptly forecasted that cyber-attacks exploiting against personal, commercial, and government infrastructure vulnerabilities would continue to increase. During conflict, the United States should expect attacks against critical defense, government, and economic infrastructure.[13] Some of the ways in which the US has sought to prepare for such attacks include: General O'Shaughnessy's proclamation, National Security Presidential Memorandum-13, "United States Cyber Operations Policy;" the work of the Cyberspace Solarium Commission, the White House's Executive Order on Improving the Nation's Cybersecurity, and National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. These have all laid the foundational steps to reduce the likelihood and impact of significant consequences from cyber-attacks against critical infrastructure.[14] They and other National cybersecurity policies and legislative reforms signify a notable shift by the federal government from the status quo.[15]

National Security Memorandum (NSM)-8, "Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems," released on January 19, 2022, is especially noteworthy. In essence, the memorandum makes Executive Order 14028 more effective.[16] Specifically, the order calls for unity of effort and collaboration between the National Manager for National Security Systems (also the Director of NSA and Commander of USCYBERCOM) and the CISA Director.[17] These new roles and responsibilities allow DoD to orchestrate cyber authorities, capabilities, and stakeholders' equities to best posture the Joint Force to detect, deter, and defeat malicious cyber-attacks targeting vulnerable critical infrastructure.[18]

Strategic Threat Assessment

Current assessments from the U.S. intelligence community indicate that peer adversaries seek to employ cyber warfare capabilities to degrade DoD networks, hold national infrastructure at risk, and delay and disrupt US ability to project forces globally.[19] Joint Force power projection is both a critical military capability and critical vulnerability as more than 80% of U.S. critical infrastructure is owned and operated by the private sector.[20] And given the open and interdependent nature of the Internet, the U.S. and other democratic nations are more susceptible to cyber-attacks against critical infrastructure than countries with restrictive Internet systems.[21] Due to these vulnerabilities and the capability of adversaries, these threats could result in significant damage across the United States, severely impacting national security.

Nation-states like Russia and China and non-state criminal actors can target and temporarily disrupt critical infrastructure with their existing cyber capabilities.[22] For example, at midnight on December 23, 2015, the Russian threat actor, Sandworm, infiltrated and shut off a Ukrainian power grid, leaving over 225,000 people without power for six hours in temperatures near zero degrees Fahrenheit.[23] This attack is even more concerning after Sandworm targeted and infiltrated U.S. energy facilities in 2014 with the malware discovered in Ukraine’s critical infrastructure cyber-attacks. It illustrates Russia’s ability to assess capabilities on other critical infrastructures before utilizing them to meet strategic objectives.[24] On July 19, 2021, the U.S. Department of Justice (DOJ) indicted four Chinese cyber actors for their illicit computer network exploitation activities targeting victims in the defense industrial base, the federal government, manufacturing, maritime, and transportation sectors, amongst others.[25] DOJ also indicted three Russian officials on March 24, 2022, for their targeted hacking campaigns against U.S. energy sector computer hardware, software, and operational technology systems between 2012 and 2017.[26] These examples highlight Russia and China’s intentions and cyberwarfare capabilities targeting U.S. critical infrastructure, enabling Moscow and Beijing to make effective defenses difficult to establish.[27]

U.S. Power Grid and Implications of Complex Catastrophes

The continental United States (CONUS) consists of three power grids – Eastern Interconnection, Western Interconnection, and Electric Reliability Council of Texas (ERCOT), as depicted in Figure 1. Three components comprise power grids: generation, transmission, and distribution.

Generation consists of traditional power plants utilizing fossil fuels, renewable power sources, and energy storage equipment for variable power sources like wind power. Transmission is the long-distance power lines and the step-up and step-down substations to transform the power for long-distance travel. Distribution consists of the assets that deliver power to the customers, private and commercial, and managed privately in regulated states.

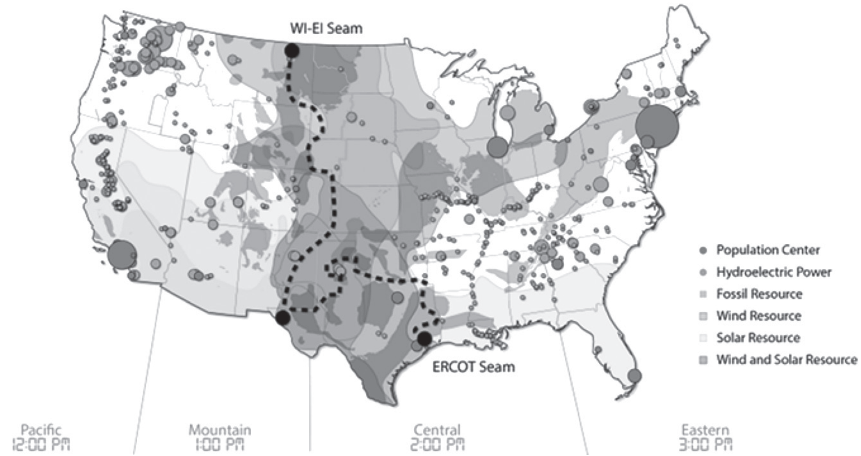


Figure 1. Continental United States' Three Power Grid Sectors[28]

The 2013 Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," identifies the energy sector as vital because it enables all critical infrastructure sectors.[29] Following a sophisticated cyber-attack, a catastrophic failure in one or more of the three grids could lead to significant casualties, especially in colder or hot climates. The hundreds of lives lost during the winter 2021 ERCOT power outage illustrate the potential impact of unmitigated power failure.[30]

A shared understanding of DoD inter- and intra-organizational relationships, roles, responsibilities, and stakeholder equities would increase preparedness across the federal government, public, and private sector. Under joint doctrine, USNORTHCOM and U.S. Indo-Pacific Command (USINDOPACOM) are responsible for "defending against, mitigating, and defeating cyberspace threats." However, only USCYBERCOM possesses the cyber expertise and intelligence apparatus to respond to such a crisis.[31] In short, USNORTHCOM and USINDOPACOM are the supported commands, and USCYBERCOM is the supporting command in complex catastrophes in the homeland.[32]

In 2012, Commander of USNORTHCOM, General Charles Jacoby, Jr., forecasted that USNORTHCOM's role could be much broader than Defense Support of Civilian Authorities (DSCA) operations.[33] During a complex catastrophe in CONUS, USNORTHCOM would likely activate one or more of its Joint Task Forces (JTFs) and execute DSCA operations following requests for assistance for cyberspace incident response, law enforcement support, or other domestic activities.[34] In particular, Defense Support to Cyber Incident Response (DSCIR) – included within the DSCA framework – authorizes the DoD to support federal departments and agencies for asset and threat response to cyber incidents outside the DoD Information Network.[35]

According to several authors, a scenario involving a cyber-attack against the U.S. power grid highlights the perennial challenges of the increasing volatility, uncertainty, complexity, and ambiguity in the current environment and forecasted future. A complex catastrophe is an intractable crisis that is predictable but not influenceable.[36] In other words, the federal government can acknowledge that a cyber-attack could occur but cannot prevent or effectively respond because required capabilities exceed those of the public and private sectors. USNORTHCOM DSCIR operations thus continually require that federal and non-federal governmental stakeholders to enumerate DoD's mission-relevant terrain in cyberspace (e.g., key servers, systems, and network infrastructure), integrate cyber response capabilities, and ensure unified action.[37]

Unified Action in Cyberspace

DoD must prepare cyber forces to, directly and indirectly, enable DSCIR operations, either directly or indirectly and for prolonged periods, because current and future challenges in cyberspace require sustained speed, agility, and ready resources. Building capability and capacity for DoD cyber protection and offensive cyberspace operations should focus on posturing forces with appropriate cyber authorities and knowledge of stakeholders equities. Cyber forces must effectively collaborate with federal government, public, and private stakeholders as cyber authorities and capability employment may require support or advocacy from these entities.

Unified action in cyberspace requires USNORTHCOM to synchronize and coordinate USCYBERCOM, CISA, and other federal and non-federal entities' cyber authorities and capabilities to achieve unity of effort before and throughout a complex catastrophe.[38] As many DoD mission functions rely on privately-owned information technology companies (e.g., cloud computing, Internet service providers, and global supply chain), DoD must build trust with these companies since the military has no direct authority over them.[39] General Nakasone recognizes this challenge and is actively working to bridge the gap by engaging with industry, academia, and international partners to establish bidirectional information exchanges to prevent and bolster the nation's defenses against cyberthreats, including launching the NSA Cybersecurity Collaboration Center in 2021 and expanding the USCYBERCOM Under Advisement program.[40]

The unregulated information environment makes people more susceptible to misinformation, propaganda, and/or radicalization, and this poses additional challenges in DoD's efforts to counter and thwart adversaries' attempts to exploit critical infrastructure vulnerabilities. This misinformation may negatively impact DoD cyberspace operations with public and private sector stakeholders.[41] Throughout a complex catastrophe and DSCA response operations, an adversary could launch an influence campaign to sow fear, doubt, and confusion amongst the American people. In addition to the impacts of denial, degradation, disruption, or destruction of critical infrastructure, foreign and domestic mis- or disinformation could erode the public trust vital for the federal government and DoD to respond to and restore cyber and infrastructure security. For example, attacks on media outlets could cause news blackouts and impede the federal government's ability to communicate directly with citizens, sowing additional uncertainty and fear.[42] USCYBERCOM could support here as it increases its efforts to link cyberspace operations with information operations more tightly.[43]

To make timely and accurate decisions concerning these events, commanders require the necessary information and intelligence to coordinate with other DoD, the federal government, and public and private sector stakeholders. Commanders' staff and subordinate commanders must rapidly and accurately capture, manage, process, and act upon the deluge of data and information to enable decision-making throughout a complex catastrophe, as illustrated in Figure 2.

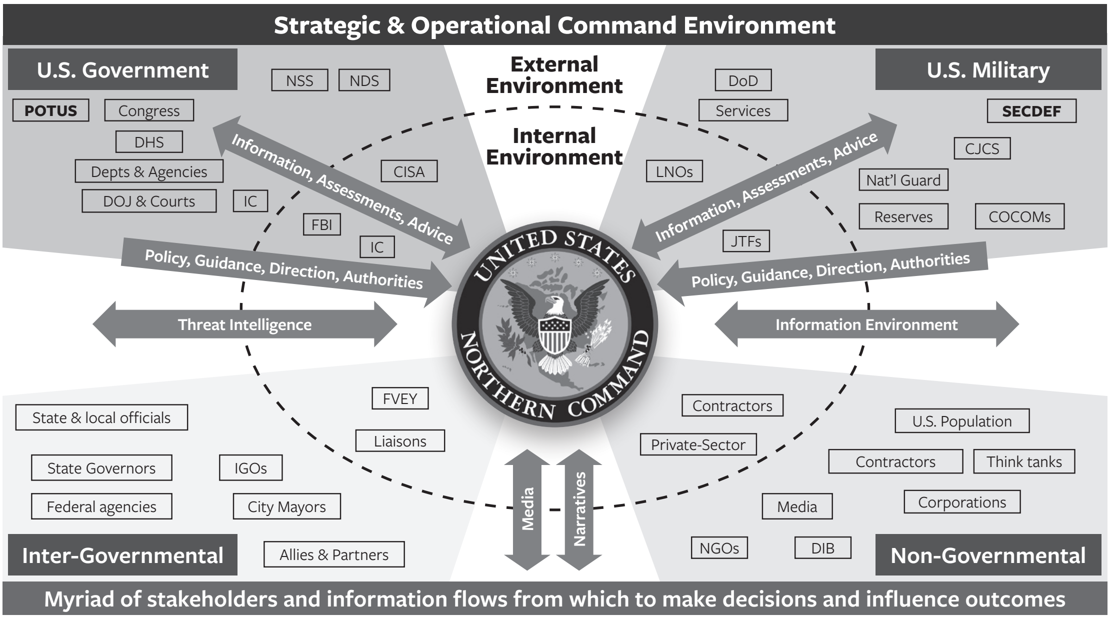


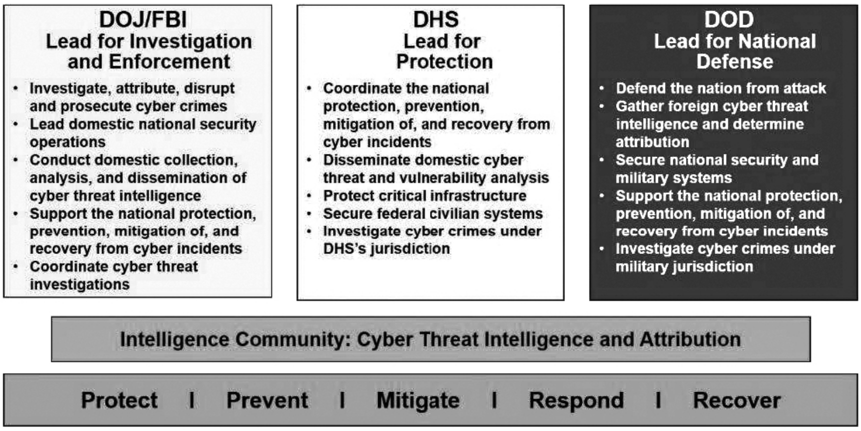
Figure 2. Complex Catastrophe Information Flows and Stakeholders[44]

Joint Force commanders, planners, and cyber forces must integrate across the diplomatic, informational, military, economic, finance, intelligence, and law enforcement instruments of national power in various arrangements of supported and supporting relationships. This level of coordination requires a firm understanding of each governmental agency's current cyberspace authorities and a great emphasis on the information and intelligence instruments in the initial hours and days of the complex catastrophe. Additionally, public and private sector stakeholders also require timely cyber threat intelligence information. Rapid detection and attribution of malicious cyber activity efforts enable the federal government, allies, and partners to leverage appropriate authorities to expel adversaries from network infrastructure and impose costs on them.[45]

According to the U.S. Department of State, when allied and partner nations contribute, attribution becomes more impactful to deterrence and legitimizes responsive actions.[46] Critical intelligence-sharing between the U.S. and Ukraine exposed Russia's malign intentions before its 2022 invasion of Ukraine. When Russian forces began deploying on Ukraine’s borders in late 2021, USCYBERCOM deployed a “hunt team” to collaborate with mission partners and “gain critical insights that have increased homeland defense for both the United States and Ukraine.”[47] Overall, unified action enhances DoD's ability to deter and respond to cyber threats and attacks with speed and agility.[48]

Cyber Mission Force Authorities to Defend the Homeland

Suppose DoD's “defend forward” operations should fail.[49] In that case, adversaries penetrating America's borders with a sophisticated cyber-attack against the U.S. power grid would impact energy, banking, finance, transportation, communication, and the defense industrial base.[50] The DoD will respond to a catastrophe of this type as outlined in Presidential Policy Directive-41, “United States Cyber Incident Coordination.”[51] Specifically, USCYBERCOM’s Cyber National Mission Force teams would detect, deter, and, if necessary, defeat adversaries in cyberspace. Cyber protection teams would also hunt for adversaries in DoD networks and non-DoD mission partners or critical infrastructure networks.[52] The Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) authorized USCYBERCOM to enable Joint Force and Interagency partners – namely DHS, the Department of Energy, and the FBI – to work on energy infrastructure security.[53] Given its mission to defend the homeland, USNORTHCOM must have a shared understanding of command relationships and authorities with USCYBERCOM, CISA, and the FBI. This clarity will enable USNORTHCOM to coordinate and deconflict cyber forces’ operations with other interagency activities.



DOJ/FBI
Lead for Investigation and Enforcement

- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS
Lead for Protection

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS’s jurisdiction

DOD
Lead for National Defense

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction

Intelligence Community: Cyber Threat Intelligence and Attribution

Protect I Prevent I Mitigate I Respond I Recover

Figure 3. National Cybersecurity Roles and Responsibilities[54]

As depicted in Figure 3, DoD's (i.e., USNORTHCOM and USCYBERCOM) close coordination with DHS/CISA and the greater interagency and intelligence community would enable cyber forces to detect, target, attribute and respond to complex cyber-attacks against the homeland. For example, USCYBERCOM's operations following adversaries' attacks against the Colonial Pipeline and José Batista Sobrinho (JBS) U.S.A. beef plants in 2021 demonstrated the successful level of coordination required between these agencies.[55] During these events, DoD contributed directly and indirectly to the intelligence community's attribution processes; hence, sound information-sharing and knowledge management activities – key components of cyberspace joint targeting coordination – were effectively executed.[56] Likewise, Joint Force cyberspace operations planners must clearly understand capabilities, requirements, operational limitations, liaisons, and legal considerations to optimize intelligence coordination.[57]

Looking externally, USNORTHCOM – in partnership with USCYBERCOM – must build consensus with decision-makers and public and private sector stakeholders before, during, and after a complex catastrophe. As outlined in Figure 4, USNORTHCOM and DoD cyber forces must understand and leverage several titles of the U.S. Code when collaborating with stakeholders to detect, deter, and defeat cyber-attacks against the U.S. power grid and other critical infrastructure.[58]

U.S. Code – U.S. Government Cyberspace Operations Authorities
Continental U.S. Complex Cyber-Attack Response Planning Considerations (USNORTHCOM)

- **Title 6 (Domestic Security) –** Assigns the Secretary of Homeland Security statutory authority to secure U.S. cyberspace.
  - In addition to USCYBERCOM's authority to enable DHS/CISA Title 6 cybersecurity efforts, cyber forces assigned to USNORTHCOM could partner with DHS/CISA in a supported and supporting capacity.
- **Title 10 (Armed Forces) –** Assigns the Secretary of Defense statutory authority to organize, train, and equip U.S. forces for military operations in cyberspace.
  - USCYBERCOM and USNORTHCOM should ensure the adequate capability and capacity of supporting cyber forces and liaison officers, and routinely validate Request for Forces packages.
- **Title 18 (Crimes and Criminal Procedure) and Title 28 (Judiciary and Judicial Procedure) –** Assigns the Attorney General statutory authority to conduct crime prevention, apprehension, and prosecution of criminals operating in cyberspace.
  - In addition to USCYBERCOM's authority to enable DOJ/FBI Title 18 cybersecurity efforts, cyber forces assigned to USNORTHCOM could partner with DOJ/FBI in a supported and supporting capacity.
- **Title 32 (National Guard) –** Statutory authority for Army and Air National Guard forces to conduct domestic consequence management.
  - The National Guard operates under Title 10 authorities if activated for federal service.
  - State governors may employ National Guard CPTs in a State Active Duty status at a state governor's direction, non-Title 10 or 32.
- **Title 40 (Public Buildings, Property, and Works) –** Statutory authority for all federal departments and agencies to establish and enforce standards for the acquisition and security of information technologies.
  - USNORTHCOM and supporting cyber forces should collaborate with federal government critical infrastructure stakeholders via Title 40, leveraging other titles under the U.S. Code (e.g., Titles 6, 10, 32).
- **Title 44 (Public Printing and Documents) –** Statutory authority for all federal departments and agencies to perform activities outlined in DoD Instruction, 8530.01, Cybersecurity Activities Support to DoD Information Network Operations.
  - USNORTHCOM and supporting cyber forces should collaborate with DoD stakeholders via Title 44, leveraging other titles under the U.S. Code.
- **Title 50 (War and National D**efense**) –** Statutory authority for Commands, Services, and agencies under the DoD and intelligence community agencies aligned under the Office of the Director of National Intelligence to secure U.S. interests by conducting military and foreign intelligence operations in cyberspace.
  - USNORTHCOM and supporting cyber forces should work and collaborate with the intelligence community, leveraging other titles under the U.S. Code.

Figure 4. United States Code and DoD Cyberspace Operations Authorities[59]

In addition to USNORTHCOM and DoD cyber forces leveraging the above authorities and respective federal agencies to counter, blunt, and actively defend the homeland in cyberspace, aspects of Title 10 and 18 warrant additional analysis. First, Chapter 13 of Title 10 (also known as the "Insurrection Act") and the Robert T Disaster Relief and Emergency Assistance Act grant the President of the United States to use the Armed Forces to help restore public order.[60] Next, Section 1835 of Title 18, the Posse Comitatus Act (PCA), prohibits the use of the U.S. military in civilian law enforcement.[61] However, homeland defense is a Constitutional exception to the PCA.[62] Thus, USNORTHCOM and supporting cyber forces can leverage Title 18 and the PCA to coordinate DoD cyber response operations with DOJ/FBI. Further, the Computer Fraud and Abuse Act of 1986 permits U.S. law enforcement and intelligence agencies to conduct lawfully authorized activities and does not constrain military cyber operations.[63]

The U.S. Cyberspace Solarium Commission made considerable progress between 2019 and 2021 in removing national cybersecurity legislative barriers. As of 2022, notable milestones included 1) the establishment, nomination, and confirmation of a National Cyber Director; 2) provisions to strengthen CISA; 3) codification of Sector Risk Management Agencies; 4) establishing a Joint Cyber Planning Office; and 5) a force structure assessment of the U.S. Cyber Mission Force. Furthermore, the President's Budget Request included $20 million to establish a Cyber Response and Recovery Fund to support asset-response activities and provide technical assistance following the declaration of a "cyber state of distress" by the Secretary of Homeland Security, in consultation with the National Cyber Director.[64] Despite this progress, laws such as the Defense Production Act and Federal Power Act may hinder DoD's cyber protection operations as private sector entities or public utilities may be reluctant to join or refrain altogether from efforts to mitigate dependencies on foreign-sourced information and communications technology and remediating cybersecurity vulnerabilities under the federal government's direction.[65]

Given these dynamics and new legislation, USNORTHCOM, its JTFs, and supporting cyber forces must remain aware of and sensitive to private and public stakeholders' interests and find common ground. Private and public entities primarily tend to the prosperity and success of their enterprises, while the federal government focuses on the US and its security. Additionally, private companies have global business partnerships and work with federal and non-federal entities.[66] International business relations can put U.S. companies in tricky situations, making decisions that may accommodate one entity but offend another. In short, establishing shared trust between the DoD, federal government, and public and private sector stakeholders is complex but essential in protecting and defending critical infrastructure.[67]

In addition to its ongoing "Shields Up" campaign – launched during Russia's build-up for its invasion of Ukraine – CISA has taken significant steps to build trust, including creating the Joint Cyber Defense Collaborative (JCDC) in August 2021, following provisions outlined within the FY 2021 NDAA. The goals of the JCDC are to "unify defensive actions and drive down risk in advance of cyber incidents occurring" and "strengthen the nation's cyber defenses through planning, preparation, and information sharing."[68] Key U.S.-based, non-governmental JCDC partners include Microsoft, Google Cloud, Amazon Web Services, and cybersecurity providers, such as CrowdStrike, Mandiant, Palo Alto Networks, Cisco, and Symantec.[69] Additionally, Congress' passage of cyber incident-reporting legislation on March 11, 2022, enables CISA to collaborate and receive cyber threat intelligence reports from the private sector to protect, defend, and respond to cyber-attacks on critical infrastructure.[70] Sharing information makes good business sense due to the cost of adversarial attacks and legal impacts affecting public and private sector organizations. Most notably, due to the potential cyber-attacks by Russia in retaliation for the US response to the invasion, US Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act into law on March 15, 2022. The Act requires owners and operators of critical infrastructure to report cyber incidents to CISA within 72 hours and ransomware demands within 24 hours.[71] The new cyber reporting law takes effect when

> CISA promulgates rules to define the entities within the critical infrastructure sectors that will be impacted by [the] law and the types of substantial cyber incidents it covers. The [law] requires CISA to issue a notice of proposed rulemaking on these definitions within 24 months from the date of the bill's enactment and issue a final rule within 18 months of issuing the proposed rule.[72]

In addition to developing a shared understanding of CISA and other federal cyber authorities, the Joint Force and federal and state governments should capitalize on the capabilities of the National Guard and Reserve cyber forces. According to Lieutenant General Jon Jensen, Director of the Army National Guard, forces gain mission-relevant experience as they rotate through USCYBERCOM in a Title 10 status.[73] USCYBERCOM also benefits from these rotations since most National Guard and Reserve members perform cybersecurity in their civilian jobs and bring great perspectives and knowledge. Their operational experience should be leveraged to build and strengthen ties between their home stations and local governments and public and private sector entities where they live and work, thereby building strategic depth, one of General Nakasone's objectives.[74]

Before, during, and after a complex catastrophe, the relationships built by National Guard and Reserve cyber personnel are foundational for improving coordination and cooperation. Guard and Reserve forces can function as primary liaisons between DoD and others concerned with cybersecurity, improving shared understanding and building trust. National Guard cyber protection teams would conduct initial cyber incident response operations in a State Active Duty status under the direction of a state governor.[75] Regardless of status, USNORTHCOM should routinely seek opportunities to leverage Title 10 cyber authorities with Title 32 authorities to activate National Guard and Reserve members during complex catastrophe cyber mission rehearsal exercises.

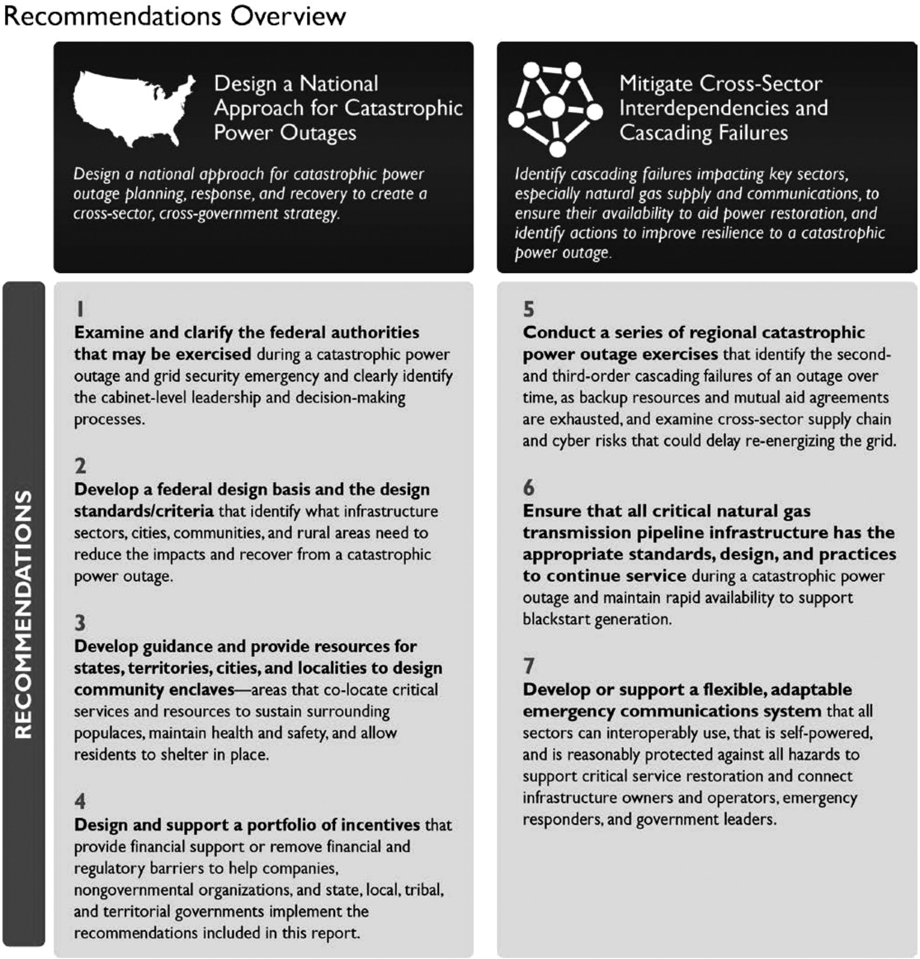
Protecting U.S. critical infrastructure from cyber-attacks primarily rests with CISA, but DoD has limited cyber authorities within the public and private sectors. However, General Nakasone's new role as the National Manager puts NSA on equal footing for providing recommendations to the Secretary of Defense, the Director of National Intelligence, and the Committee on National Security Systems to improve the detection of cyber incidents affecting these systems.[76] Combined NSA and CISA authorities, capabilities, insights, and partnerships enhance USNORTHCOM DSCIR and DoD cyber force operational readiness.

*Orchestrating Authorities, Capabilities, and Equitie*s

As the DoD continues building capability and capacity to detect, deter, and defeat cyberspace threats against the homeland, it should expect resistance from external federal government and public and private sector entities. The Services may also push back given their focus on modernization plans, budget prioritization, and operations abroad. Thus, a DoD "Complex Catastrophe Cyber Stakeholders, Communications, Authorities, and Narratives" (C3 SCAN) framework could assist USNORTHCOM and USCYBERCOM in effectively planning, prioritizing, and executing complex catastrophe DSCIR operations.[77]

This framework could serve as an information and knowledge management tool, enabling the Office of the Secretary of Defense to facilitate DoD cyberspace communication and collaboration with CISA and other public and private sector stakeholders.[78] The DoD C3 SCAN accounts for the local contexts of each stakeholder that could be involved, including their cyber equities, authorities, primary communications channels, and stakes in DoD's mission-relevant terrain in cyberspace. It also accounts for stakeholders' and organizations' roles in USNORTHCOM DSCIR operations.[79] The C3 SCAN would capture the various information flows, means, and narratives that serve as tools for guiding DoD senior leaders' strategic communications and key leader engagements with stakeholders, including allies and partner nations. Former USNORTHCOM Deputy Commander and National Infrastructure Advisory Council (NIAC) member, retired Lieutenant General Reynold Hoover, emphasizes open communications, strategic messaging, and engagement with key critical infrastructure stakeholders for effective response operations in the homeland.[80]

USNORTHCOM, its JTFs, and supporting cyber forces know the various cyber authorities necessary to work with and through its various partners in different situations. Section 6 of Executive Order 14028 directed DHS (i.e., CISA) to "develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activity respecting [Federal Civilian Executive Branch] Information Systems."[81] Through persistent engagement with mission partners, USNORTHCOM and supporting cyber forces could participate in stakeholders' meetings and working groups to review and update their respective National cybersecurity incident response playbooks, orders, and campaign plans. The primary aims of the C3 SCAN are to 1) identify DoD cyber advocates and opponents; 2) build trust and a shared understanding amongst stakeholders regarding cyber authorities, capabilities, and equities; and 3) identify and register stakeholders' concerns and DSCIR requirements. Due to increasing cyber threats posed by malign actors, especially Russia and China, national and international networks' vulnerabilities and complex interrelationships demand immediate coordinated action at all levels.[82] Collaboration and work should also center on discovering and capitalizing on shared equities and interests to build more resilient relationships for crisis management. For example, in 2018, the NIAC provided the National Security Council with whole-of-nation response recommendations for improving US ability to prepare for and recover from catastrophic power outages, as depicted in Figure 5.[83]



Recommendations Overview

Design a National Approach for Catastrophic Power Outages

Design a national approach for catastrophic power outage planning, response, and recovery to create a cross-sector, cross-government strategy.

Mitigate Cross-Sector Interdependencies and Cascading Failures

Identify cascading failures impacting key sectors, especially natural gas supply and communications, to ensure their availability to aid power restoration, and identify actions to improve resilience to a catastrophic power outage.

RECOMMENDATIONS

1
Examine and clarify the federal authorities that may be exercised during a catastrophic power outage and grid security emergency and clearly identify the cabinet-level leadership and decision-making processes.

2
Develop a federal design basis and the design standards/criteria that identify what infrastructure sectors, cities, communities, and rural areas need to reduce the impacts and recover from a catastrophic power outage.

3
Develop guidance and provide resources for states, territories, cities, and localities to design community enclaves—areas that co-locate critical services and resources to sustain surrounding populaces, maintain health and safety, and allow residents to shelter in place.

4
Design and support a portfolio of incentives that provide financial support or remove financial and regulatory barriers to help companies, nongovernmental organizations, and state, local, tribal, and territorial governments implement the recommendations included in this report.

5
Conduct a series of regional catastrophic power outage exercises that identify the second- and third-order cascading failures of an outage over time, as backup resources and mutual aid agreements are exhausted, and examine cross-sector supply chain and cyber risks that could delay re-energizing the grid.

6
Ensure that all critical natural gas transmission pipeline infrastructure has the appropriate standards, design, and practices to continue service during a catastrophic power outage and maintain rapid availability to support blackstart generation.

7
Develop or support a flexible, adaptable emergency communications system that all sectors can interoperably use, that is self-powered, and is reasonably protected against all hazards to support critical service restoration and connect infrastructure owners and operators, emergency responders, and government leaders.

Figure 5. National Infrastructure Advisory Council Recommendations for Surviving a Catastrophic Power Outage, December 2018[84]

Over time, USNORTHCOM and supporting cyber forces will improve their credibility with constituents and stakeholders. They should exercise and rehearse the communications mechanisms identified within the C3 SCAN during table-top and large-scale exercises such as CISA's biennial Cyber Storm exercise and other whole-of-nation exercises.[85] After these events, USNORTHCOM should review and refine the C3 SCAN's communications means, capabilities, and authorities. Additionally, the Command should update all cyber-related orders and directives and continuously exchange liaison officers with USCYBERCOM, DHS/CISA, and DOJ/FBI. Finally, DoD key leader engagements should engender creative ideas and discussions, bolster buy-in, and create greater transparency between stakeholders. Organizing and conducting these liaison events ahead of time is one method of mitigating the effects of intractable crises, even if the scope and scale of a future complex catastrophe are unknown.[86]

CONCLUSION

As revisionist powers seek to disrupt the international order and conduct operations below the level of armed conflict, including cyber-attacks, DoD must effectively position its cyber forces and capabilities to defend against cyber-attacks before they hit the homeland.[87] An attack against the U.S. power grid could result in multiple failures in life-sustaining infrastructure and significantly impact Joint Force power-projection capabilities.[88] Accordingly, USNORTHCOM must work closely with USCYBERCOM to collaborate with CISA and other federal and non-federal stakeholders' cyber authorities, capabilities, and equities to posture DoD cyber forces to respond with speed and agility. Current federal cyber laws, such as the Defense Production Act, Federal Power Act, and others, may hinder USNORTHCOM and supporting cyber forces' ability to conduct cyberspace operations in defense of the homeland. However, several titles in the U.S. Code (e.g., Title 10, 32, 50) and recent years' NDAAs equip the USNORTHCOM Commander to effectively command and control cyber defensive operations and support USCYBERCOM's offensive operations (e.g., joint targeting) before, during, and after a complex catastrophe.[89] Still, close partnerships and education must continuously occur to deconflict or clarify conflicts or inconsistencies in the numerous laws and U.S. Code.

As the supported command during complex catastrophes within CONUS, USNORTHCOM must possess a shared understanding of command relationships, cyber authorities, and capabilities with USCYBERCOM before, during, and after a complex cyber-attack. Well-coordinated national cybersecurity response planning will enable USNORTHCOM to validate plans and orders, enumerate and prioritize mission-relevant terrain in cyberspace, and ensure DSCIR readiness.[90] Preparation should include USNORTHCOM routinely exchanging liaison officers with USCYBERCOM, CISA, and the FBI and leveraging Title 10 and 32 authorities to activate National Guard and Reserve forces to prepare DoD organizations and personnel for their roles in these crises. Overall, the combined authorities, capabilities, and insights of USCYBERCOM, NSA, and the National Manager are a force-multiplier in enabling USNORTHCOM, CISA, and DoD cyber forces to thwart complex cyber-attacks.

Finally, tools such as the DoD C3 SCAN could enable the USNORTHCOM and USCYBERCOM Commanders and cyber forces to orchestrate CISA, interagency, intelligence community, public, and private sector cyber authorities, capabilities, and equities in a complex catastrophe to plan and prioritize DSCIR options. In 1942, innovative civil-military collaboration enabled the U.S. military to partner with the newly established Civil Air Patrol to protect America's sea lanes, defend against and deter future U-Boat attacks, and thwart Germany's Operation Drumbeat.[91] Similarly, the combined authorities, capabilities, and partnerships of DoD, CISA, the FBI, and the public and private sector can enable cyber forces to thwart asymmetric attacks against the homeland.

NOTES

1. The President's National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, 3, https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.
2. Ed Offley, "The Burning Shore: How Hitler's U-Boats Brought World War II to America," (Basic Books, New York, 2014), 103-131; and Deputy Secretary of Defense, *Definition of the Term Complex Catastrophe, Memorandum for Secretaries of the Military Departments,* Washington, D.C., February 19, 2013, https://info.publicintelligence.net/DoD-ComplexCatastropheDefinition.pdf.
3. Ibid, 127-133.
4. Michael Gannon, "Operation Drumbeat: The Dramatic True Story of Germany's First U-Boat Attacks Along the American Coast in World War II," (Harper & Row Publishers, New York, 1990), 343; and Richard Lentinello, *How Gas Rationing Worked During World War II*, December 30, 2019, https://www.hemmings.com/stories/2019/12/30/how-gas-rationing-worked-during-world-war-ii.
5. Ibid, 343.
6. Lennart Maschmeyer and Nadiya Kostyuk, *There is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict*, February 8, 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/; and Michael Hull, *Operation Drumbeat's Devastating Toll on Allied Shipping*, December 12, 2018, https://warfarehistorynetwork.com/2018/12/09/operation-drumbeats-devastating-toll-on-allied-shipping/.
7. Nicole Sganga, *"It's Coming": President Biden Warns of "Evolving" Russian Cyber Threat to U.S.,"* March 21, 2022, https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/; and Raphael Satter, Zeba Siddiqui, and James Pearson, *"U.S. warns China could hack infrastructure, including pipelines, rail systems*," May 26, 2023, https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/.
8. Cybersecurity and Infrastructure Security Agency (CISA), *Shields Up,* https://www.cisa.gov/shields-up. Accessed February 11, 2022.
9. U.S. Cyberspace Solarium Commission, *Final Report*, v, https://www.solarium.gov/home, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed February 10, 2022.
10. General Paul Nakasone, *CYBERCOM and NSA Chief: Cybersecurity is a Team Sport,* December 6, 2021, https://www.defensenews.com/outlook/2021/12/06/cybercom-and-nsa-chief-cybersecurity-is-a-team-sport/.
11. Department of Homeland Security, *National Preparedness Goal,* https://www.dhs.gov/national-preparedness-goal. Accessed February 10, 2022. "The National Preparedness Goal defines what it means for the whole community to be prepared for all types of disasters and emergencies. The goal itself is succinct: 'A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.' These risks include events such as natural disasters, disease pandemics, chemical spills and other man-made hazards, terrorist attacks and cyber-attacks."
12. Kyle Rempfer, '*The Homeland is No Longer a Sanctuary' Amid Rising Near-Peer Threats, NORTHCOM commander says,* August 27, 2018, https://www.militarytimes.com/news/your-air-force/2018/08/27/the-homeland-is-no-longer-a-sanctuary-amid-rising-near-peer-threats-northcom-commander-says/.
13. Department of Defense, 2022 National Defense Strategy, 5, 8, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.
14. The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ and *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/; U.S. Cyberspace Solarium Commission; and The CSC 2.0 Project, *Preserving the Legacy and Continuing the Work of the Cyberspace Solarium Commission,* https://www.cybersolarium.org/. Accessed February 10, 2022.
15. Senators Angus King and Tom Fannin, *To Combat Cyber-Attacks, the US Government and Businesses Must Work More Closely*, July 19, 2021, https://www.cnn.com/2021/07/19/perspectives/cyber-attacks-security-us-government-businesses/index.html. "The commission recommended more than 75 measures ... 25 of the commission's proposals passed into law;" U.S. Cyberspace Solarium Commission, see "Our Progress"; and Solarium Commission *2021 Annual Report on Implementation*, August 2021, https://www.solarium.gov/public-communications/2021-annual-report-on-implementation.

NOTES

16. The White House, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems.
17. Tim Frank, *National Security Memorandum/NSM-8: A Call to Action on Defense Systems,* January 24, 2022, https://www.splunk.com/en_us/blog/industries/national-security-memorandum-nsm-8-a-call-to-action-on-defense-systems.html.
18. The White House, *National Cyber Strategy of the United States of America*, September 2018, specifically pillar #1: "protecting the American people, homeland, and way of life by safeguarding networks systems, functions and data," https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; and Department of Defense, *Summary of the Department of Defense Cyber Strategy 2018,* specifically goal #2: "compete and deter in cyberspace" and #3: "strengthen alliances and attract new partnerships."
19. U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World,* July 14, 2016, 17, 24, 26, 35, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917; General Glen VanHerck, *Statement of Commander, United States Northern Command and North American Aerospace Defense Command Before the House Armed Services Committee and Subcommittee on Strategic Forces*, March 8, 2023, 9, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/NNC_FY23%20Posture%20Statement%20%20HASC%20SF%20FINAL.pdf; and insights from retired Army Lieutenant General and former USNORTHCOM Deputy Commander (2016-2018), Reynold Hoover, to the author, February 23, 2022.
20. Reynold Hoover; and Steve Lasky, *A Rise In Ransomware Threatens America's Critical Infrastructure,* January 25, 2021, https://www.securityinfowatch.com/cybersecurity/article/21228250/a-rise-in-ransomware-threatens-americas-critical-infrastructure.
21. Ministry of Defence, *Global Strategic Trends: The Future Starts Today,* 6th ed. (United Kingdom: Ministry of Defence, Strategic Trends Programme: Development, Concepts and Doctrine Centre, October 2018), 134, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf; and as defined by the U.S. Joint Chiefs of Staff (JCS) in Joint Publication (JP) 3-12, *Joint Cyberspace Operations* (Washington DC: U.S. Joint Chiefs of Staff, December 19, 2022), "Cyberspace. A global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers;" https://jdeis.js.mil/jdeis/new_pubs/jp3_12.pdf.
22. Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, February 6, 2023), 10, 15, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf; and VanHerck, *Statement of Commander* ...9-10.
23. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; Dragos, *Crashoverride: Analysis of the Threat to Electric Grid Operations* (Hanover, Md.: Dragos, 2017), 10, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf; and Dustin Volz, *U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage*, February 25, 2016, https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.
24. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar;" and Serhiy Martynets, *U.S. Suspects Russia of Involvement in Cyber-attacks on Ukrainian Power Grids* (Ukrainian National News), January 7, 2016, https://www.unn.com.ua/uk/news/1536191-ssha-pidozryuyut-rosiyu-u-prichetnosti-do-kiberatak-na-ukrayinski-elektromerezhi.
25. Cybersecurity and Infrastructure Security Agency, Alert (AA21-200A) *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Departmen*t, July 19, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-200a.
26. Federal Bureau of Investigation, *Four Russian Government Employees Charged in Two Separate Hacking Campaigns Targeting Worldwide Critical Infrastructure,* March 24, 2022, https://www.fbi.gov/news/stories/russian-government-employees-charged-in-hacking-campaigns-032421.
27. Office of the Director of National Intelligence, Annual Threat Assessment ...,10, 15; and Satter, *"U.S. warns China could hack infrastructure, including pipelines, rail systems."*

NOTES

28. Office of Energy Efficiency and Renewable Energy (EERE), *East Meets West? Lab Study Focuses on Connecting Power Grid from Coast to Coast* (Washington, DC: EERE, May 31, 2017), https://www.energy.gov/eere/articles/east-meets-west-lab-study-focuses-connecting-power-grid-coast-coast; and U.S. Energy Information Administration, *U.S. Electric System is Made Up of Interconnections and Balancing Authorities*, July 20, 2016, https://www.eia.gov/todayinenergy/detail.php?id=27152; In Figure 1, "The Eastern Interconnection encompasses the area east of the Rocky Mountains and a portion of northern Texas. The Eastern Interconnection [EI] consists of thirty-six balancing authorities: thirty-one in the United States and five in Canada. The Western Interconnection [WI] encompasses the area from the Rockies west and consists of 37 balancing authorities: thirty-four in the United States, two in Canada, and one in Mexico. The Electric Reliability Council of Texas (ERCOT) covers most, but not all, of Texas and consists of a single balancing authority."
29. Cybersecurity and Infrastructure Security Agency, *Energy Sector*, https://www.cisa.gov/energy-sector and https://www.cisa.gov/critical-infrastructure-sectors. Accessed March 16, 2022); and The White House, *Presidential Policy Directive - Critical Infrastructure Security and Resilience*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
30. Loch Johnson, "On Drawing a Bright Line for Covert Operations," American Journal of International Law, Vol. 86, No. 2 (April 1992), 286, 292, https://doi.org/10.2307/2203235. According to Lennart Maschmeyer, Johnson's escalation ladder does not include critical infrastructure sabotage, but the scope of effects places it within the riskiest, "extreme options"; and Peter Aldhous, Stephanie M. Lee and Zarah Hirji, *The Texas Winter Storm and Power Outages Killed Hundreds More People Than the State Says*, May 26, 2021, https://web.archive.org/web/20210718121413/https:/www.buzzfeednews.com/article/peteraldhous/texas-winter-storm-power-outage-death-toll.
31. U.S. Joint Chiefs of Staff, Joint Publication (JP) 3-27, *Homeland Defense* (Washington DC: U.S. Joint Chiefs of Staff, April 10, 2018), II-8, II-12, II-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf. This paper primarily focuses on a potential complex catastrophe (i.e., a complex cyber-attack) occurring within the continental U.S.
32. Ibid, vii – viii, II-6, 10-11.
33. Cheryl Pellerin, *NORTHCOM Prioritizes Homeland Defense, Cyber*, Partners (U.S. Strategic Command), March 14, 2012, https://www.stratcom.mil/Media/News/News-Article-View/Article/983560/northcom-prioritizes-homeland-defense-cyber-partners/.
34. U.S. Joint Chiefs of Staff, JP 3-28, *Defense Support of Civil Authorities* (Washington DC: U.S. Joint Chiefs of Staff, October 29, 2018), I-2, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf; and JP 3-27, *Homeland Defense,* II-10.
35. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum (DTM) 17-007 – "Interim Policy and Guidance for Defense Support to Cyber Incident Response*, June 21, 2017 (change 6, June 21, 2023), 2, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-007.pdf.
36. Jonathan Ablett and Andrew Erdmann, "Strategy, Scenarios, and the Global Shift in Defense Power," McKinsey & Company, April 2013, 1, http://www.mckinsey.com/insights/public_sector/strategy_scenarios_and_the_global_shift_in_defense_power; and Stephan Gundel, "Towards a New Typology of Crises," Journal of Contingencies and Crisis Management 13, no. 3 (2005), 112.
37. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, I-3; Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum ...*, 9-11; and Eric Pederson, MAJ Don Palermo (USA), MAJ Stephen Fancey (USA), LCDR (Ret) Tim Blevins, *DOD Cyberspace: Establishing a Shared Understanding and How to Protect It*, January 1, 2022, https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.
38. U.S. Joint Chiefs of Staff, JP 3-08, *Interorganizational Cooperation* (Washington DC: U.S. Joint Chiefs of Staff, October 12, 2016, validated October 18, 2017), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08.pdf; JP 3-33, *Joint Task Force Headquarters* (Washington DC: U.S. Joint Chiefs of Staff, 31 January 2018).
39. Lasky, A Rise in Ransomware; and U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, IV-17.
40. Nakasone, *CYBERCOM and NSA Chief*; and Martin Matishak, "*Cyber Command to expand 'canary in the coal mine' unit working with private sector,"* June 28, 2023, https://therecord.media/cyber-command-under-advisement-team-cyber-threat-collaboration.
41. Ministry of Defence, *Global Strategic Trends*, 16, 81, 124.

NOTES

42. Dmitri Alperovitch, *How Russia Has Turned Ukraine Into a Cyber-Battlefield*, January 28, 2022, https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield.
43. Mark Pomerleau, *Cyber Command Moving Toward an Integrated Information War Approach,* March 11, 2022, https://www.fedscoop.com/cyber-command-moving-toward-an-integrated-information-warfare-approach/.
44. Adapted from General Raymond Odierno Knowledge Management Workshop product, May 2011. Modifications to graphic and addition of USNORTHCOM logo created by the author.
45. General Paul Nakasone, *Statement of Commander, U.S. Cyber Command Before the 118th Congress Senate Committee on Armed Services*, March 7, 2023, 4, https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf.
46. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*, Officer of the Coordinator for Cyber Issues, May 31, 2018, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.
47. Major Sharon Rollins, *Defensive Cyber Warfare Lessons from Inside Ukraine*, U.S. Naval Institute Proceedings, Vol. 149/6/1,444, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine; Patrick O'Nell, T*he US is Unmasking Russian Hackers Faster Than Ever: The White House Was Quick to Publicly Blame Russia For A Cyberattack Against Ukraine, The Latest Sign That Cyber Attribution is a Crucial Tool in the American Arsenal*, February 21, 2022, https://www.technologyreview.com/2022/02/21/1046087/russian-hackers-ukraine/; John Grady, *Intel Sharing Between U.S. and Ukraine 'Revolutionary' Says DIA Director,* March 18, 2022, https://news.usni.org/2022/03/18/intel-sharing-between-u-s-and-ukraine-revolutionary-says-dia-director; and General Paul Nakasone, *Statement of Commander, U.S. Cyber Command Before the 118th Congress Senate Committee on Armed Services*, March 7, 2023, 4, https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf.
48. U.S. Cyberspace Solarium Commission …, v.
49. Paul M. Nakasone, "A Cyber Force for Persistent Operations," Joint Force Quarterly, 92 (2019), 12-13, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.
50. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, III-16.
51. U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, III-I-2.
52. Cohen, *CYBERCOM and NSA Chief*; and U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, II-8.
53. Cohen, *CYBERCOM and NSA Chief*.
54. U.S. Army War College, *Strategic Cyberspace Operations Guide,* Center for Strategic Leadership, August 1, 2021, 60, https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.
55. Julian Barnes, *U.S. Military Has Acted Against Ransomware Groups, General Acknowledges,* December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.
56. U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations*, IV-8-11.
57. Ibid, IV-2, IV-23.
58. FindLaw, *United States Code – Unannotated,* January 1, 2018, https://codes.findlaw.com/us/; U.S. Joint Chiefs of Staff, JP 3-27, Homeland Defense …, III-3. United States Code; and Cornell Law School, 6 *U.S. Code § 466 - Sense of Congress Reaffirming the Continued Importance and Applicability of the Posse Comitatus Act*, https://www.law.cornell.edu/uscode/text/6/466.
59. Figure created by the author; derived from U.S. Joint Chiefs of Staff, JP 3-12, *Joint Cyberspace Operations* …, III-3 ("Key Titles of United States Code Related to Cyberspace Operations"); FindLaw, *United States Code – Unannotated,* January 1, 2018, https://codes.findlaw.com/us/; Cornell Law School, 6 U.S. Code § 466; and Congressional Research Service, *National Guard Civil Support in the District of Columbia*, February 23, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11768.
60. U.S. Code, §251. *Federal Aid for State Governments*, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section251-1&num=0&edition=prelim. Accessed March 3, 2022.
61. Peter Pascucci and Kurt Sanger, *Revisiting a Framework on Military Takedowns Against Cybercriminals*, July 2, 2021, https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals.
62. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense,* I-6; and Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum*, 3.

NOTES

63. U.S. Army War College, *Strategic Cyberspace Operations Guide, 106-111; U.S. Department of Justice, 9-48.000-Computer Fraud and Abuse Act*, https://www.justice.gov/jm/jm-9-48000-computer-fraud. Accessed March 3, 2022); Cornell Law School, 6 U.S. Code § 466; and the Honorable Paul Ney, Jr., *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.
64. The CSC 2.0 Project, 2021 *Annual Report on Implementation,* 23-24, https://drive.google.com/file/d/19V7Yfc5fvEE6dG-IoU_7bidLRf5OvV2__/view.
65. U.S. Cyberspace Solarium Commission, ..., 63, 69; Department of Homeland Security, *Defense Production Act*, https://www.fema.gov/disaster/defense-production-act. Accessed February 10, 2022); and Congressional Research Service, The *Legal Framework of the Federal Power Act*, January 22, 2020, https://crsreports.congress.gov/product/pdf/IF/IF11411.
66. Neil Jenkins, *Testimony Before the US-China Economic and Security Review Commission on U.S. Private Industry Responses to the China Cyber Challenge*, February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/Neil_Jenkins_Testimony.pdf.
67. King and Fannin, *To Combat Cyber-Attacks.*
68. Cybersecurity and Infrastructure Security Agency, *Shields Up; and Joint Cyber Defense Collaborative*, https://www.cisa.gov/jcdc. Accessed February 18, 2022.
69. Jenkins, *Testimony Before the US-China Economic and Security Review Commission.*
70. Cybersecurity and Infrastructure Security Agency, *Statement From CISA Director Easterly on the Passage of Cyber Incident Reporting Legislation*, March 11, 2022, https://www.cisa.gov/news/2022/03/11/statement-cisa-director-easterly-passage-cyber-incident-reporting-legislation; and Jen Easterly @CISAJen Twitter update, March 11, 2022, https://twitter.com/CISAJen/status/1502254277301002244.
71. Shardul Desai, et al, *Cyber Incident Reporting Requirements for Critical Infrastructure Sectors Signed into Law*, March 16, 2022, https://www.hklaw.com/en/insights/publications/2022/03/cyber-incident-reporting-requirements-for-critical-infrastructure.
72. Desai, *Cyber Incident Reporting Requirements for Critical Infrastructure Sectors.*
73. Army War College, Military Strategy and Campaigning (Lesson 11) Homeland Defense/DSCA Moderated Panel, January 3, 2022.
74. Nakasone, *Statement of Commander*, 5-6; and Cohen, *CYBERCOM and NSA Chief;* and Army Cyber Command @ARCYBER, tweet regarding Army Reserve and National Guard openings in cyber, signal, legal, intelligence, logistics, IT and security, March 2, 2022, https://twitter.com/ARCYBER/status/1499074555180109834.
75. Reynold Hoover; and *New York State Division of Military and Naval Affairs, New York National Guard Job Zone, Cyber Protection Team (CPT) Temporary Duty (M-Day)*, https://dmna.ny.gov/jobs/?id=cpt#:~:text=The%20Cyber%20Protection%20Team%20is%20a%20joint%20partnership,basis%2C%20in%20support%20of%20state%20and%20federal%20missions. Accessed March 3, 2022.
76. The White House, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.*
77. The author developed the DoD "C3 SCAN" framework which can be accessed here: https://warroom.armywarcollege.edu/wp-content/uploads/22-039-DoD_C3_SCAN_Framework.png.
78. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum,* 7-9.
79. Department of Defense, *Deputy Secretary of Defense Directive-Type Memorandum,* 13-14.
80. Reynold Hoover, *Lecture: Military Operations in CONUS* (Part of the Strategic Landpower Integrated Research Project), Army War College, February 16, 2022.
81. Cybersecurity and Infrastructure Security Agency, *New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*, November 2021, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
82. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, II-3.
83. The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (Arlington, Virginia: CISA NIAC, December 2018), 2, https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf.

NOTES

85. The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage*, 3.
85. Cybersecurity and Infrastructure Security Agency, *CISA Hosts Eighth Cyber Storm Exercise With More Than 200 Organizations*, March 14, 2022, https://www.cisa.gov/news/2022/03/14/cisa-hosts-eighth-cyber-storm-exercise-more-200-organizations; https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise; and The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage*, 3.
86. Gundel, "Towards a New Typology of Crises," 112.
87. Jim Garamone, *Global Integration Seeks to Buy Leaders Decision Time, Increase 'Speed of Relevance',* July 2, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1565240/global-integration-seeks-to-buy-leaders-decision-time-increase-speed-of-relevan/.
88. VanHerck, *Statement of Commander*, 9.
89. U.S. Joint Chiefs of Staff, JP 3-27, *Homeland Defense*, II-13.
90. VanHerck, *Statement of Commander*, 5,9.
91. Offley, "The Burning Shore," 157-158; Gannon, "Operation Drumbeat," 343; and Hap Harris, "Civil Air Patrol," *Aerospace Historian*, Vol. 13, No. 4 (Winter 1966), 186, https://www.jstor.org/stable/44524484. Accessed January 15, 2022.