

4-7-2022

Contested Deployment

Bert B. Tussing

John Eric Powell

Benjamin C. Leitzel

Follow this and additional works at: <https://press.armywarcollege.edu/monographs>



Part of the [Defense and Security Studies Commons](#), [Emergency and Disaster Management Commons](#), [Military and Veterans Studies Commons](#), [Other Public Affairs](#), [Public Policy and Public Administration Commons](#), [Policy Design, Analysis, and Evaluation Commons](#), [Politics and Social Change Commons](#), [Public Administration Commons](#), [Public Affairs Commons](#), and the [Public Policy Commons](#)

Recommended Citation

Bert B. Tussing, John Eric Powell, and Benjamin C. Leitzel, *Contested Deployment* (Carlisle, Pennsylvania: US Army War College Press, 2022),
<https://press.armywarcollege.edu/monographs/948>

This Book is brought to you for free and open access by USAWC Press. It has been accepted for inclusion in Monographs, Collaborative Studies, & IRPs by an authorized administrator of USAWC Press.

INTEGRATED RESEARCH PROJECT

CONTESTED DEPLOYMENT

Project Directors

Bert B. Tussing
John Eric Powell
Benjamin C. Leitzel

Contributing Researchers

James L. Boling, Jonathan M. Boling, John J. Borek
Charles P. Brady, John Bretthorst, Stephen W. Ladd
Steven E. Landis, Edmund "Beau" Riely
Arthur C. Roscoe, Brian D. Wisniewski

**DECISIVE
POINT**

The USAWC Press Podcast Companion Series

<https://ssi.armywarcollege.edu/decisive>

STRATEGIC STUDIES INSTITUTE

CONTESTED DEPLOYMENT

A US Army War College Center for Strategic Leadership Integrated Research Project

Bert B. Tussing
John Eric Powell
Benjamin C. Leitzel

Project Directors

James L. Boling
Jonathan M. Boling
John J. Borek
Charles P. Brady
John Bretthorst
Stephen W. Ladd
Steven E. Landis
Edmund "Beau" Riely
Arthur C. Roscoe
Brian D. Wisniewski

Contributing Researchers

April 2022

The views expressed in this publication are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the US Government. Authors of Strategic Studies Institute and US Army War College Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official US policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is cleared for public release; distribution is unlimited.

This publication is subject to Title 17 United States Code § 101 and 105. It is in the public domain and may not be copyrighted by any entity other than the covered author.

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and US Army War College Press, US Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5244.

This is a peer-reviewed publication. The views expressed in this publication are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the US government. Authors of Strategic Studies Institute and US Army War College Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official US policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is cleared for public release; distribution is unlimited.

This publication is subject to Title 17 United States Code § 101 and 105. It is in the public domain and may not be copyrighted by any entity other than the covered author.

Comments pertaining to this publication are invited and should be forwarded to: Director, Strategic Studies Institute and US Army War College Press, US Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5244.

ISBN 1-58487-835-5

Cover Photo Credits

The front and back covers have been designed using resources from Freepik.com: Industrial port and container yard (flipped, cropped, and used across entire cover).

US ARMY WAR COLLEGE CENTER FOR STRATEGIC LEADERSHIP

The Center for Strategic Leadership provides strategic education, ideas, doctrine and capabilities to the Army, the Joint Force, and the Nation. The Army, Joint Force, and national partners recognize the Center for Strategic Leadership as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.

US ARMY WAR COLLEGE PRESS

The US Army War College supports the US Army War College by publishing monographs and a quarterly academic journal, *Parameters*, focusing on geostrategic issues, national security, and Landpower. US Army War College Press materials are distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities. The US Army War College serves as a bridge to the wider strategic community.

TABLE OF CONTENTS

Chapter 1. Introduction.....	1
Chapter 2. Army Deployments in a Contested Homeland: A Framework for Protection.....	7
Chapter 3. Strategic Seaports and National Defense in a Contested Deployment.....	21
Conclusion	33
Chapter 4. Single Point of Failure.....	35
Prevention	36
Protection.....	38
Mitigation	41
Recovery	48
Conclusion.....	50
Chapter 5. The Interstate Highway System: Reinvestment Needed Before a Contested Deployment.....	53
Background of the Interstate Highway System	54
Use of the Interstate Highway System Today in a Contested Deployment	56
Current Condition of US Roads and Bridges	57
Interstate Highway System Vulnerabilities.....	58
Gray-Zone Activities.....	59
Terrorism	61
Recommendations.....	63
Conclusion.....	66
Appendix A: Contested Deployment Cyber Index.....	67
Appendix A-1: Cyberspace Defense of Critical Infrastructure: Legal and Policy Limitations.....	71
Overview of Defense Support of Civil Authorities (DSCA)	72

Current DSCA Policies Regarding Cyberspace Support.....	77
Protected Critical Infrastructure Information Program.....	79
National Cyber and Communications Information Integration Center	80
Infrastructure Policy and Regulation Issues in the Private Sector	81
Recommendations	83
Conclusion.....	84
Appendix A-2: Framework for a Critical Infrastructure Cyber Resilience Assessment.....	87
Appendix A-3: Command and Control of Domestic Cyber Response Operations in a Complex Catastrophe	103
Background.....	104
A Complex Catastrophe.....	107
Findings	116
General.....	117
National Security Council/Cyber Response Group/UCG.....	117
Joint Field Office.....	118
Joint Task Force Cyber	118
Conclusion	119
Appendix B: Impacts of Full Mobilization in the Contested Homeland	121
Historic Context	121
Contested Homeland.....	124
What Is Mobilization?	127
Gaps in Full Mobilization Planning, Exercises, and Regulations	129
What We Do Not Know Might Hurt Us.....	130
Recommendations.....	132

Conclusion134

Appendix C: Acronyms and Abbreviations.....137

About the Researchers.....141

FOREWORD

The American way of war in the twentieth century required the ability to project combat power effectively onto foreign shores from a homeland reasonably secure from adversarial threats. Using the current doctrinal terminology, the homeland was the core strategic support area from which US forces could mobilize, deploy, employ, and sustain combat power against enemies abroad.

Expectations surrounding future warfare with a near-peer adversary leave little hope for such unfettered power projection. The current strategic environment suggests US forces will face contested deployment from enemies possessing the capabilities to obstruct and disrupt kinetically and virtually.

Infrastructure critical to ensuring power projection is aging and easily susceptible to attack. Processes and procedures critical for these functions are only partially under the control of the military. Civil-military coordination requirements will span federal, state, and local government, transforming the extant paradigm from Defense Support of Civil Authorities to Civil Support of Military Activities.

This study, undertaken in 2018 for an integrated research project headed by the Homeland Defense and Security Issues Group of the Army War College Center for Strategic Leadership, contributes to the thinking that will be required to prepare US forces—and, especially, the US Army—for “contested deployment.” While acknowledging a broad swath of issue areas, the study focuses predominantly on physical infrastructure issues that will impact the ability of the United States to mobilize, deploy, employ, and sustain its forces. While the study’s findings and recommendations are not always intuitive when compared to effective business practices, they promote a necessary redundancy made urgent by the threat of determined nation-state opponents or their proxies.



COLONEL JAKE LARKOWICH
Director
Center for Strategic Leadership

SUMMARY

Early in academic year 2018, a group of US Army War College faculty and students came together in pursuit of an integrated research project devoted to an examination of contested deployment and the growing realization the US homeland can no longer be considered an inviolable zone in preparing for war. Expecting free movement of forces in mobilization, movement to ports of embarkation, and deployment against the nation's adversaries is beneath reason. Two oceans and benevolent neighbors to the north and south can no longer be considered a significant buffer against internal and external enemies. Adversaries of the United States will seek to disrupt or disable the movement of its forces long before they can be placed in combat against foes overseas, and the nation must be prepared for this opposition.

Gray zone activities, hybrid warfare, and the obfuscation of the boundaries between competition and conflict signal a new urgency for examinations such as this one. This study is not exhaustive; the participants made a conscious decision to limit their examination to a few – albeit immediate – physical considerations among the challenges US forces would most likely face when moving “from fort-to-port.”

The study begins with a discussion of the fundamentals of contested deployment. Current doctrine and recent events, from the COVID-19 pandemic to social unrest, focus attention on Department of Defense support to civil authorities. In a contested deployment scenario, planners and policymakers need to consider the ways in which the coordination process would work when the military needs the support of state, local, tribal, and territorial resources to overcome adversaries' obstacles to deployment. Next, the study continues with an examination of the 22 US strategic seaports, identifying issues ranging from throughput to security and the structural integrity of port infrastructure.

Infrastructure readiness is not limited to seaports. Thus, an examination of the current state of the Interstate Highway System, its criticality to successful deployment, and the vulnerabilities that can be exploited by adversaries follows. Then, a review of munition production and distribution and the vulnerabilities of the business model that sustains the employment of US forces is provided.

Many other issues require the military's attention in general and the US Army's attention in particular. One set of issues, for instance, is addressed by Professor Ben Leitzel of the Army War College's Center for Strategic Leadership in an integrated research project recommending ways in which Department of Defense cyber units might respond to a cyberattack on critical infrastructure supporting the deployment of forces. Similarly, a paper written by Lieutenant Colonel Stephen W. Ladd (US Army Reserve), while a member of the US Army War College class of 2018, addresses the critical issue of mobilizing the reserve component. Ladd introduces difficulties that could be encountered if the complex issues surrounding mobilization are exacerbated by deliberate obstructions that are predictable in a contested deployment environment. Both of these studies are included as appendices to this study.

The realization the homeland can no longer guarantee a secure space for mobilization and deployment is recognized in current defense strategy and evolving Army doctrine. The observations, issues, and recommendations in this study are this US Army War College team's contribution to the next step—realistically preparing for and addressing the disruption or disabling of US forces during mobilization.

CHAPTER 1. INTRODUCTION

Future deployment activities within the homeland during large-scale multi-domain operations (MDO) will require close civil support to military activities to ensure the generating force can sustain and project forces to various operational theaters. Evolving MDO doctrine identifies the homeland as the core strategic support area (SSA)—“the area of cross-combatant command coordination, strategic sea and air lines of communications, and the homeland.”¹ Future adversaries will seek to disrupt and degrade the United States’ ability to move personnel and materiel through the battlefield framework from homeland basing to the forward fight. This chapter expands the discussion of contested deployment operations within the SSA.

We define contested deployment as deployment operations faced with incidental, inadvertent, or deliberate obstruction, resulting in a prohibition of, or significant delay in, the relocation of forces and materiel to desired operational areas. Adversaries’ capabilities have expanded the battlefield geographically to the homeland, limiting its status as a sanctuary and impeding freedom of maneuver.² Thus, beginning planning for readiness and deployment operations within the homeland as if it were a contested environment is critical. The contested spaces discussion will cover both areas where US or coalition forces can challenge adversaries and areas where adversaries can challenge US or coalition forces to deny freedom of action.³ Only through deep engagement and dialogue about the challenges associated with this emerging operational environment can we successfully address the risks.

The emerging security environment, “more complex and volatile than any we have experienced in recent memory,” leaves little doubt the next conventional conflict we face will occur within the territorial confines of the United States.⁴ The US Army Training and Doctrine Command pamphlet, *US Army in Multi-Domain Operations 2028*, outlines a future operational environment in which state and nonstate actors will expand operations into the US homeland to disrupt US advantages.⁵ Power projection supporting combatant commands originates in the continental United States as the core SSA for the Joint Force.⁶ Therefore, in future large-scale combat operations, the United States must expect near-peer adversaries to take measures to delay, disrupt, or obstruct force-projection efforts within the homeland. Accounting for contested deployment operations in the homeland is an obligation the United States cannot ignore.

1. US Army Training and Doctrine Command (TRADOC), *The US Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: TRADOC, December 6, 2018), GL-9.

2. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States: Sharpening the Military’s Competitive Edge* (Washington, DC: Department of Defense, January 2018), 3.

3. TRADOC, *Multi-Domain Operations 2028*, GL-2.

4. Mattis, *Summary of 2018 National Defense Strategy*, 1.

5. TRADOC, *Multi-Domain Operations 2028*, iii, vi, 13.

6. TRADOC, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040* (Fort Eustis, VA: TRADOC, December 2017).

Expecting near-peer foes to allow the United States freedom of movement when mobilizing its forces is no longer reasonable. Adversaries' multi-domain capabilities across an expanded battlefield, including the homeland, must be taken into account. The chapters in this integrated research project focus on challenges to the movement of US forces, from unit installations to ports of embarkation. The chapter authors investigate key contested deployment operational topics dealing with force protection, strategic seaports, the Interstate Highway System, and the risks of translating business model efficiencies to military operations. The resulting recommendations for doctrine and policy seek to stimulate professional discussion regarding the challenges of conducting operations in the stateside SSA.

Evolving adversary capabilities mandate deployment operations within the territorial confines of the United States be a part of military planning and an evolving MDO doctrine. Future force projection operations to support combatant commands must include operational considerations for generating homeland forces within the MDO framework.⁷ The chapters of this study focus on critical components that enable fort-to-port deployment operations.⁸ Anticipating and preparing for contested operations within US borders is essential. We cannot win "over there" if we lose "over here."⁹

Charles Brady begins the second chapter by asserting the homeland has, indeed, been a virtual sanctuary during relatively recent conflicts. Persistent fear of disruption or sabotage at installations, transportation, and logistics nodes has not been felt since World War II. This fear will most likely return in the future. He suggests a contested deployment scenario would require adjustments to military and civilian coordination and cooperation mechanisms to ensure the United States' ability to deploy forces. Current regulations and doctrine provide an initial framework, but force projection operations in the homeland require more robust codified solutions to address civil support to the Department of Defense.

Brady shows civil support of military movement is a critical component during a contested scenario. In such a scenario, the Department of Defense would seek support from civil authorities, reversing conventional thinking about DoD's Defense Support of Civil Authorities mission set. He suggests revising doctrine within the Army may be a good start, but interagency and civil-military integration will be crucial for success. A mechanism for this integration may be the National Preparedness System, which Brady recommends expanding to include support to the Department of Defense in protecting installations, lines of communication, and ports of embarkation during conflict. Core documents should be revised to account for and further develop the concepts of planning, prevention, and protection encompassing critical

7. TRADOC, *Multi-Domain Operations* 2028, 13.

8. Headquarters, Department of the Army, *Army Deployment and Redeployment*, Army Techniques Publication (ATP) 3-35 (Washington, DC: Headquarters, Department of the Army, March 2015).

9. Bert Tussing and Barrett Parker, "The Multi-Domain Battle: What's in It for the Homeland?," *War Room* (blog), November 10, 2017, <https://warroom.armywarcollege.edu/articles/multi-domain-battle-whats-homeland/>.

interagency and civilian support for force projection operations.¹⁰ In closing, Brady reiterates his less-than-intuitive position that “the Army would be the supported unit instead of the supporting unit” in a contested deployment scenario.

In the third chapter, Lieutenant Colonel Arthur C. Roscoe examines America’s strategic seaports within the context of a contested deployment. His research addresses approaches for mitigating deployment delays and disruptions engineered by adversaries in addition to shortcomings caused by the posture and condition of existing seaport infrastructure. Strategic seaports are a critical force projection enabler because 90 percent of military cargo is transported by sea.¹¹ The United States currently has 22 strategic seaports, 17 of which are commercial ports the military may use to deploy resources in the event of conflict overseas.¹² While these strategic seaports have served their purpose during the past two decades of operations, they may not be satisfactory in the next war.

Citing several reports, Roscoe uncovers issues at multiple strategic seaports with throughput, structural integrity, security, operational readiness, funding, and authorities.¹³ Regarding port security, he points to substantive progress since the 9/11 attacks thanks to initiatives like the Security and Accountability for Every Port Act of 2006 and the Port Security Grant Program.¹⁴ Beyond physical concerns, he explores emerging cyber threats within the operational environment and cites the transworld malware cyberattack on the Maersk seaport terminals in June 2017, which for a time shut down operations in the Port of Los Angeles.¹⁵

In addition to the threat of cyberattacks against US seaports, Roscoe highlights the danger electromagnetic pulse weapons pose as a military option for adversaries.¹⁶ He suggests an “e-bomb,” reportedly possessed by both Russia and China, could be a

10. Department of Homeland Security, *National Response Framework*, 4th ed. (Washington, DC: Department of Homeland Security, October 28, 2019).

11. Zina D. Merritt, *Defense Logistics: The Department of Defense’s Report on Strategic Seaports Addressed All Congressionally Directed Elements*, GAO-13-511R (Washington, DC: Government Accountability Office, May 13, 2013), 1.

12. Merritt, *Defense Logistics*, 1.

13. Donna J. Simkins et al., *Port Look 2008: Strategic Seaports*, Report SDD80T1 (Tysons, VA: LMI, October 2008); and Merritt, *Defense Logistics*, 15.

14. Henry H. Willis, “Ten Years after the Safe Port Act, Are America’s Ports Secure?,” *RAND Blog*, April 6, 2016, <https://www.rand.org/blog/2016/04/attractive-targets.html>; and John D. Donahue and Mark H. Moore, eds., *Ports in a Storm: Public Management in a Turbulent World* (Washington, DC: Brookings Institution Press, 2012), 30.

15. Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017, H.R. 3101, 115th Cong. (2017).

16. *Terrorism and the EMP Threat to Homeland Security: Hearing before the Subcommittee on Terrorism, Technology, and Homeland Security of the Committee of the Judiciary*, 109th Cong. (2005) (statement of tLowell Wood, commissioner, Congressional Electromagnetic Pulse Commission).

feasible means to disrupt port operations and could cause a cascading failure throughout an entire power grid.¹⁷

In concluding the chapter, Roscoe makes several recommendations for mitigating a contested deployment scenario involving our strategic seaports. First, he calls for revising the outdated evaluation criteria used to select and designate seaports as strategic ports. Developed by the Military Surface Deployment and Distribution Command, the Army's component of US Transportation Command, Roscoe holds the current criteria is ill-suited for the emerging operational environment.¹⁸ Second, he recommends incentivizing commercial port owners to seek necessary improvements to the structural integrity of ports through grants and other programs. Finally, he suggests a joint, civil-military approach to more significant cybersecurity measures.¹⁹ Ultimately, Roscoe contends, these joint assessments of the threats, devoted to identifying clear points of failure in military deployment operations, would permit appropriate prioritization and mitigation.

In the fourth chapter, Lieutenant Colonel John Bretthorst examines points of failure related to the application of civilian business models to military operations. He maintains the military's current business-systems approach is detrimental and essentially creates vulnerabilities that manifest as single failure points. Business -model approaches that deliberately seek to eliminate redundancies may degrade the military's ability to operate effectively.²⁰ He examines this apparent dichotomy through its implications for munitions logistics and cites examples from the two main military munitions terminals—Military Ocean Terminal Concord and Military Ocean Terminal Sunny Point—to demonstrate the disadvantages associated with a pure business-model perspective.²¹

Bretthorst notes most US munitions are now stored within the homeland because of the drawdown of the US military presence in Europe and elsewhere following the

17. Jenna Baker McNeill and Richard Weitz, *Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe* (Washington, DC: Heritage Foundation, October 20, 2008); and Aylin Woodward, "Weak Links in US Power Grid Vulnerable in Event of Catastrophe," *New Scientist* (website), November 16, 2017, <https://www.newscientist.com/article/2153472-weak-links-in-us-power-grid-vulnerable-in-event-of-catastrophe/>.

18. Merritt, *Defense Logistics*, 1.

19. Department of Transportation, "US Department of Transportation Launches BUILD Transportation Program, Announces \$1.5 Billion Notice of Funding Opportunity," Department of Transportation, April 25, 2018, <https://www.transportation.gov/briefing-room/dot3218>; and Department of Homeland Security, "Fiscal Year 2017 Port Security Grant Program Fact Sheet," Maritime Security Outlook, n.d., https://www.maritimesecurityoutlook.com/images/2017_PSGP/FY_2017_PSGP_Fact_Sheet_FINAL_508.pdf.

20. Everett C. Dolman, "On the Business Models of War," *Strategy Bridge* (blog), November 22, 2017, <https://thestrategybridge.org/the-bridge/?author=56fdec1037013b09a736eeda>.

21. Kimberly Hanson, "Military Ocean Terminals Play Strategic Role in Defense," US Army, October 17, 2013, https://www.army.mil/article/113348/military_ocean_terminals_play_strategic_role_in_defense.

collapse of the Soviet Union.²² This shift in storage sites necessitates bulk movement to theaters of operation from the SSA, primarily through strategic seaports. He points out seaports, by their very nature, are vulnerable to threats from land, sea, and air.²³ In addition, Military Ocean Terminal Concord and Military Ocean Terminal Sunny Point are the only ports in the United States today capable of safely handling military munitions, thus exacerbating the vulnerability. Though the consolidation of military munitions ports advances a certain level of efficiency, this consolidation also creates a positive targeting opportunity for enemies of the United States.

Asserting munitions nodes are exceptionally susceptible assets, Bretthorst stresses the need to evaluate prevention, protection, mitigation, and recovery measures. He contends protecting the munitions infrastructure is a shared responsibility among federal, state, local, and territorial entities that requires vigilance among private- and public-sector stakeholders as a critical prevention measure.²⁴ While reducing munitions infrastructure may appear logical in the business-efficiency model, he concludes this reduction would leave the military far more susceptible to the disruption of its vital assets.

The ability of adversaries to interfere with the flow of munitions or disrupt or destroy them in place is a matter of compelling urgency. Other factors of concern are the decline in the munitions infrastructure industrial base, a reduced munitions-capable labor force, the slow mobilization process of the force, and the designation of Military Ocean Terminal Sunny Point and Military Ocean Terminal Concord as the only two vital strategic munitions ports as single points of failure.

In the fifth chapter, Lieutenant Colonel Edmund “Beau” Riely investigates risks to mobilization and deployment across the Interstate Highway System, officially designated the Dwight D. Eisenhower National System of Interstate and Defense Highways. President Eisenhower envisioned the system as a network of major highways designed to provide ease and safety in transportation, enhance the US economy, and offer a means for the military to transport equipment and personnel to ports of embarkation.²⁵ The importance of these functions has been clear since the network’s inception, leading Presidential Policy Directive 21 to designate the Transportation Systems Sector as one of the country’s 16 Critical Infrastructure Sectors.²⁶

22. Stacie L. Pettyjohn, *US Global Defense Posture, 1783–2011* (Santa Monica, CA: RAND Corporation, 2012), 83–89.

23. Keith Laing, “Lawmakers Fret about Potential Terrorist Attacks at US Ports,” *The Hill*, October 27, 2015, <https://thehill.com/policy/transportation/258290-lawmakers-fret-about-potential-terrorist-attacks-at-us-ports>.

24. Eric V. Larson and John E. Peters, *Preparing the US Army for Homeland Security* (Santa Monica, CA: RAND Corporation, 2001), 70–71.

25. Elisheva Blas, “The Dwight D. Eisenhower National System of Interstate and Defense Highways: The Road to Success?,” *History Teacher* 44, no. 1 (November 2010): 1; Tim Minahan, “Interstate Highways Pay Off,” *Purchasing* 121, no. 3 (September 5, 1996): 45; and Doug Briggs, “USTRANSCOM JDPAC/SDDC TEA” (PowerPoint presentation, 2018 Committee on Transportation System Operations Annual Meeting, Atlanta, GA, August 27–29), 11.

26. Barack Obama, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (Washington, DC: White House, February 12, 2013).

Title 32 of the Code of Federal Regulations mandates the Department of Defense integrate national defense requirements into the development, construction, and use of the public Interstate Highway System.²⁷ Riely posits the system, as one of the 16 Critical Infrastructure Sectors, must be integrated into national readiness efforts for large-scale mobilization. He identifies several vulnerabilities and concerns regarding the Interstate Highway System and expresses a common US concern: The Interstate Highway System is deteriorating. The problem is exacerbated by “increasing congestion, unprecedented levels of travel—particularly by large trucks—and insufficient funding to make needed repairs.”²⁸ If left unfixed, these deficiencies will undermine the ability of US forces to deploy. Riely notes the physical and structural trends the deficiencies represent create vulnerabilities that can be easily exploited by multi-domain-capable adversaries.

Disruption across the Interstate Highway System could seriously interrupt deployment operations, whether as a function of physical or cyberactivities. Riely warns against the potential impact of US adversaries’ information operations designed to foment disorder in the guise of transportation-related labor strikes and protests.²⁹ Another set of exploitable vulnerabilities he explores is the transportation of hazardous materials along the highway system. Chemical and petroleum shipments are the most concerning because they are the most prevalent hazardous materials transported on US roadways.³⁰ The absence of a uniform regulatory authority that deals with the transportation of chemicals and petroleum among states is disconcerting in the best of times. Adding this daily misfunction to the potential for a deliberate attack should move US discomfort past dangerous to ominous.

Riely offers straightforward measures to mitigate the threats to the Interstate Highway System. For example, he recommends immediate attention be paid to repairing and revitalizing the system, a challenge he acknowledges can only be met by Congress. Next, realizing the challenge requires greater civilian-military coordination, Riely proposes the National Guard Bureau and the Department of Homeland Security create a team to explore preparation for and countering of contested deployment threats. For the hazardous materials issue, he recommends the Department of Homeland Security establish and enforce a hazardous materials quality-control standard akin to the one provided by the National Association of Chemical Distributors.³¹ Finally, in a measure incorporating public response and government initiative, he calls for the development of

27. Transportation Engineering Agency, “Highways for National Defense (HND),” Military Surface Deployment and Distribution Command, n.d., <https://www.sddc.army.mil/sites/TEA/FunctionsSpecialAssistant/Pages/HighwaysNationalDefense.aspx>.

28. Mark S. Kuhar, “Interstate Highway System Turns 60,” *Rock Products* 119, no. 7 (July 2016): 88.

29. Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for US Military Strategy* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2016), 41; and Charles R. Burnett et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2016), 29.

30. Mary A. Field, “Highway Security and Terrorism,” *Review of Policy Research* 21, no. 3 (May 2004).

31. “Responsible Distribution,” National Association of Chemical Distributors, n.d., <https://www.nacd.com/rd/about/>.

a national-level hotline, accompanied by interstate digital signage and other advertising means, to increase awareness and provide for prevention simultaneously.

Ultimately, this integrated research project is designed to contribute to the discussion of homeland contested deployment operations within the MDO framework. The project does not serve as a comprehensive listing of all issues or challenges the United States may face and is not prescriptive in addressing them. The goal of the project was to highlight the issues and collectively assess the threats and the ability of the United States to meet them. Ultimately, the United States must take a proactive, rather than reactive, approach to addressing the threat of contested deployment.

2. ARMY DEPLOYMENTS IN A CONTESTED HOMELAND: A FRAMEWORK FOR PROTECTION

Even in a permissive environment, military deployments are contested by the sheer difficulty of getting people, equipment, and supplies moving in unison and on time. During marshaling and movement to ports of embarkation, fog and friction provide plenty of resistance and set the stage for even more to come once operations begin at a deployed location. Traditionally, unit movements from the United States occur, if not in a stress-free environment, then at least in a relatively threat-free environment. What happens when we add an adversary who is contesting our deployment to the workload? Does the US Army have a plan for contested deployment?

This chapter examines the necessary military and civil-military procedures, processes, policies, and relationships for ensuring the United States' ability to deploy forces within the homeland while the deployment is being contested by an active threat. It also identifies the challenges and obstacles of contested deployment and recommends planning and preparation actions for the Army to succeed with a primary focus on a planning framework for protection, which is an essential joint function critical for deploying in a contested environment. Specifically, the chapter examines how the Army must provide for its security and plan for additional protection support from civil authorities.

The definition of "protection" is the "[p]reservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area."¹ The plan for protecting a deploying force and providing the critical support it needs calls for a change in mindset by both the Army and the nation. War is changing, the threat is changing, and the United States and its Army need to adapt to these changes. The *2018 National Defense Strategy* and many other current strategic documents identify this fact. The *Summary of the 2018 National Defense Strategy of the United States* states, "It is now undeniable that the homeland is no longer a sanctuary. America is a target. . . . During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."² The United States must plan and prepare to mobilize and operate in this environment. Policymakers can use existing Army and Department of Homeland Security doctrine and procedures to inform much of this planning and preparation. With a basic framework for protection, the military can adapt and focus more on the execution of deployment operations.

Current Army doctrine for protection and security covers deployed (that is, in-theater) operations (Army Doctrine Publication 3-37, *Protection*) and the garrison environment (Army Regulation 525-2, *The Army Protection Program*).³ In a contested

1. Chairman of the Joint Chiefs of Staff (JCS), *DOD Dictionary of Military and Associated Terms* (Washington, DC: Chairman of the JCS, 2021), 174.

2. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge* (Washington, DC: DoD, January 2018), 3.

3. Headquarters, Department of the Army (HQDA), *Protection*, Army Doctrine Publication (ADP) 3-37 (Washington, DC: HQDA, July 2019); and HQDA, *The Army Protection Program*, Army Regulation 525-2 (Washington, DC: HQDA, December 8, 2014).

deployment, these protection activities are vital to the survival of the force. These two Army force protection and continuity-of-operations activities must overlap and become operational (that is, tactically focused, as in a warfighting mode) to protect the force and ensure mission-essential functions occur. Beyond organic Army capabilities for protection, external support will also be required in a contested, fort-to-port scenario. Given the increased threat, local, state, and federal authorities, as well as Joint Force organizations, will be needed to a greater extent than is currently the case.

The protection framework discussed in this chapter applies to more than just protection for the deploying force. The findings and recommendations apply to protecting computers and networks, essential operations, infrastructure, emergency management and response, health support, policing, security of information, and installation property. The protection framework and the Army Protection Program (APP) concept extend to other support and response functions required in the deployment process, such as transportation, staging, and convoy control. The larger issue is how the Army and the nation must adapt the current operational paradigm and doctrine to meet the requirements of a contested deployment.

At this stage in our nation's war on violent extremism, or violent extremism's war on our nation, the idea the Army could be attacked inside US borders should not be a surprise.⁴ Events since the 9/11 attacks, such as the Boston Marathon bombers in April 2013 or the truck driver who mowed down cyclists and pedestrians in New York City in October 2017 after being inspired by the Islamic State of Iraq and Syria, are reminders our homeland is contested. These incidents are not random. The mayhem has a purpose. The enemy is no longer at the gates—it is within them. Servicemembers in the heartland are targets, whether they are gunned down by a homegrown violent extremist at recruiting stations in Chattanooga, Tennessee, or hunted on the Internet by the Islamic State of Iraq and Syria.⁵ The *US Army Operating Concept* describes a war in which “enemy organizations *expand* operations to the US homeland. Enemies and adversaries will operate beyond physical battlegrounds, and enemies will subvert efforts through infiltration of US and partner forces (e.g., insider threat) while using propaganda and disinformation to effect public perception.”⁶

Targeted and purposeful attacks will continue. The Army has adapted in the past and must continue to adjust to these changing conditions to ensure deploying soldiers and the enablers they require are protected. Realistically, a whole-of-government response is required, and civil authorities and other governmental organizations with homeland security responsibilities will be needed. Domestic agencies and government organizations that traditionally call on the military for support for

4. Mattis, *Summary of 2018 National Defense Strategy*, 3.

5. Kristina Sgueglia, “Chattanooga Shootings ‘Inspired’ by Terrorists, FBI Chief Says,” CNN, December 16, 2015, <https://www.cnn.com/2015/12/16/us/chattanooga-shooting-terrorist-inspiration/index.html>; and Dugald McConnell and Brian Todd, “Purported ISIS Militants Post List of 1,400 US ‘Targets,’” CNN, August 13, 2015, <https://www.cnn.com/2015/08/13/world/isis-militants-american-targets/index.html>.

6. US Army Training and Doctrine Command (TRADOC), *The US Army Operating Concept: Win in a Complex World 2020–2040*, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: TRADOC, October 7, 2014), 10.

domestic emergencies may take on tasks to support the military, whose focus will be on national security missions overseas.⁷ The US military has entered a new era, and this fact cannot be emphasized enough. To quote the director of the Homeland Defense and Security Issues Group at the US Army War College, “Preparations for battle must begin in the homeland. The home front will probably be part of the next major battlefield, and the price of poor preparation will be paid by soldiers and civilians alike. To ensure US forces are organized, trained, equipped, and postured, we must develop battle concepts that consider the domestic battlefield. We cannot win ‘over there’ if we lose ‘over here.’ ”⁸

The threat to a deployment could range from irregular attacks by small units or single individuals intending to disrupt and terrorize servicemembers to even more sophisticated attacks against critical infrastructure. Enemy forces in the homeland contesting a deployment may attack port facilities, bridges, or highways used to transport troops and equipment.⁹ Our adversaries could launch cyber or electromagnetic attacks to “disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.”¹⁰ These threats will be persistent, coordinated, diffused, and focused on the military and its deployment effort. The Army recognizes this new challenge, and through decisive action and adapting its protection and civil-military doctrine, it can meet and defeat the threats which attempt to “counter US power projection . . . limit US freedom of action . . . overwhelm defense systems, and impose a high cost on the United States to intervene in a contingency or crisis.”¹¹

The framework for protecting the Army in a contested homeland is Army Regulation 525-2, *The Army Protection Program*.¹² This regulation establishes the protection architecture and processes Army-wide for installation security, safety, emergency response, and for maintaining mission-essential functions under duress from natural or man-made causes.¹³ The Army Protection Program, the Army’s initial layer in the homeland for the protection of forces, families, critical infrastructure, and functions in a challenged environment, provides the starting point for securing Army activities, including deployment. The challenge to operationalizing this doctrine will be doing so under potential combat conditions inside the borders of the United States.

7. Department of the Army, *Defense Support of Civil Authorities*, ADP 3-28 (Washington, DC: Department of the Army, July 26, 2012), 3.

8. Bert Tussing and Barrett Parker, “The Multi-Domain Battle: What’s in It for the Homeland?,” *War Room* (blog), November 10, 2017, <https://warroom.armywarcollege.edu/articles/multi-domain-battle-whats-homeland/>.

9. Mattis, *Summary of 2018 National Defense Strategy*, 3.

10. Donald Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), 12.

11. TRADOC, *US Army Operating Concept*, 10.

12. HQDA, *Army Protection Program*.

13. HQDA, *Army Protection Program*, 7.

Typically, Army installations and outlying sites containing reserve or National Guard units execute APP procedures and protective measures in a steady-state mode, free of adversarial threats. Drills confirm emergency response procedures, and real-world emergencies are thankfully few and relatively short in duration. The APP processes are born from experiences and lessons learned at installations worldwide in different scenarios. The processes evolve over time, keep pace with changes in threats, and safeguard the force and the fort. The program, founded on the core Army values of leadership, protection, and mission accomplishment, exists so Army communities and their operations can withstand the shock of a real-world hazard. The Army's response to the 2009 active-shooter incident at Fort Hood, Texas, illustrates these principles in the face of a deadly attack and confirmed the importance of the Army's installation protection procedures and responses that saved lives, now detailed in the Army Protection Program.¹⁴ Painful lessons learned from this incident were incorporated into Army Regulation 525-2, which was published in 2014.

The *Fort Hood Army Internal Review Team: Final Report* identified key actions that were essential to the fort's resilience in the face of a lethal assault.¹⁵ The processes used by the post, along with others developed over time, have been captured in the regulation. Fort Hood continued operations, provided safety and security to its tenants, and effectively coordinated with civil authorities to respond and care for soldiers in the midst of an emergency.¹⁶ The Army's first layer of security exists by virtue of the *Army Protection Program*. With planning and preparation, this framework is a good starting point for protecting a deploying force facing resistance.

The features of the Army Protection Program, for which the assistant secretary of the Army (manpower and reserve affairs) and the deputy chief of staff, G-3/5/7, have the lead, include 12 functional and three enabling areas. Figure 2-1 shows how the execution of Army missions are supported by the Army Protection Program.¹⁷ The program is a starting point for the daunting task of protecting the Army in the homeland and enabling the force to deploy. Headquarters, Department of the Army, directs the program, which manages "risks relative to the safety and security of our Soldiers, civilians, family members, contractors, facilities, infrastructure, and information."¹⁸ The purpose of the program is to protect against threats to a domestic Army and to enable mission-essential functions in an environment in which an adversary has the "intent, capability, and opportunity to cause loss or damage."¹⁹

14. Fort Hood Army Internal Review Team, *Fort Hood Army Internal Review Team: Final Report* (Washington, DC: US Army, August 4, 2010).

15. Fort Hood Army Internal Review Team, *Final Report*.

16. Fort Hood Army Internal Review Team, *Final Report*.

17. HQDA, *Army Protection Program*, 8.

18. HQDA, *Army Protection Program*, i.

19. HQDA, *Army Protection Program*, 7, 37.

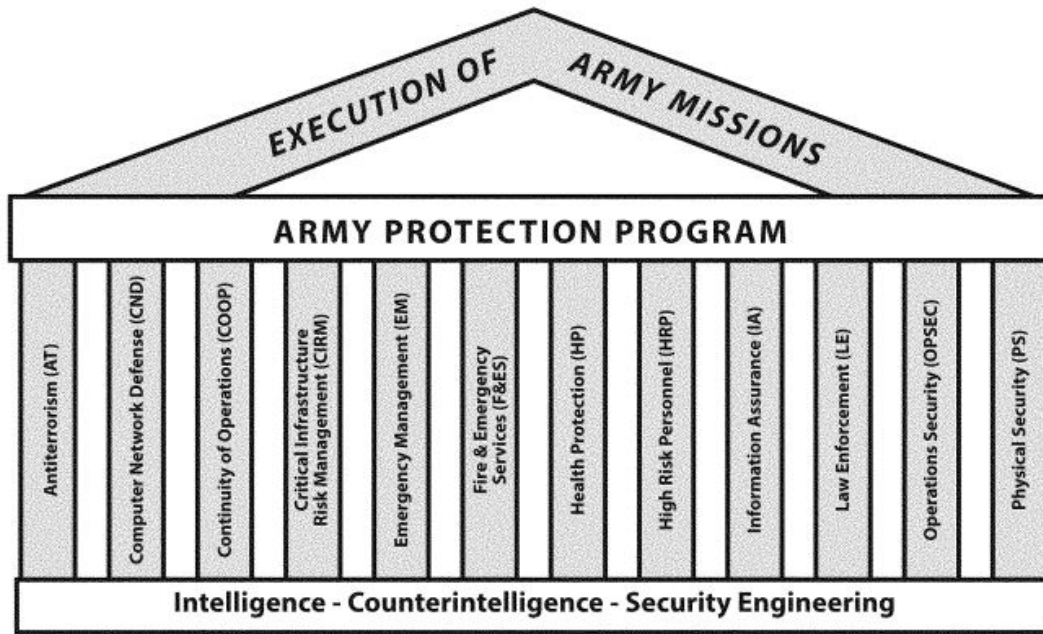


Figure 2-1. Army Protection Program functional elements and enabling functions

In theory, the program is prepared to deal with all hazards, assuming it is applied, sufficiently manned, and adequately resourced to meet its requirements. To achieve these tasks, the APP doctrine or its implementing regulation must incorporate other scenarios, such as future threats that may be envisioned. The program must recognize the changing character of war and how it will affect base protection functions. This new environment will most likely present an evolving range of threats of increasingly greater magnitude and persistence of which will gradually increase. Heightened kinetic activity with a longer duration and greater lethality will require scaling up the Army Protection Program to meet the demand of such a scenario.

The 12 functional and three enabling areas cover the spectrum of vulnerability for a contested deployment scenario.²⁰ For protection from likely deployment threats, the antiterrorism functions in the program direct “a collective, proactive effort focused on the prevention and detection of terrorist attacks against Department of Defense personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment.”²¹ Enabling the 12 functional elements are intelligence and counter-intelligence, criminal intelligence, and security engineering. These functions are familiar in a warfighting scenario, which a contested deployment would most likely resemble. The entire construct of protection, as outlined in Army Regulation 525-2, can be adapted to the future threats the United States is likely to face at home stations. The Army Protection Program must be adapted, and then operationalized, to face this environment and protect the Army’s maneuvers to ports of embarkation.

20. HQDA, *Army Protection Program*, 21-25.

21. HQDA, *Army Protection Program*, 21.

The challenge for a garrison commander and staff will be to execute and sustain the program in a contested scenario. Achieving adequate levels of resources and expertise will probably be a challenge. The APP framework must evolve to provide for protection and continuity of operations during a contested deployment and exercises involving a contested deployment scenario. As the regulation states, to be effective, the garrison must conduct an “exercise that simulates a real event as closely as possible . . . to evaluate integrated capabilities in a highly stressful environment that simulates actual conditions . . . [and] tests capabilities, exercises most functions, . . . coordinate[s] the efforts of several organizations, and [stands up] the Emergency Operations Center.”²²

Although the Army Protection Program is robust in scope and intent and has been proven to protect soldiers, installations, and essential services and functions under adverse conditions, garrison forces will likely need more resources and manning in a contested homeland scenario.²³ Funding to provide for additional security supplies and services, overtime for civilians, and additional soldiers to man potentially around-the-clock operations must be produced. As will be discussed later, soldiers from the deploying force can be incorporated into the protection functions to augment APP requirements. For sustained and adequate support, however, the garrison commander has the responsibility per the program to coordinate with Headquarters, Department of the Army, which can contact the Department of Defense, Joint activities, and federal agencies for additional support.²⁴ The requirements for providing this kind of security and ongoing support will be extensive. Envisioning this scenario and testing garrison capabilities will clarify the way ahead for providing the resources required for garrison forces supporting a deploying force attempting to maneuver to ports of embarkation.

The counterpart guidance to the Army Protection Program is Army Doctrine Publication 3-37, *Protection*, which addresses a deployed, tactical environment.²⁵ In a contested deployment in an insecure homeland, deploying forces must activate this function sooner than they may expect. Linking these two protection activities with the available forces from both garrison and deploying units will facilitate an integrated shield of protection.

This Army doctrine publication is capable guidance for protecting forces in contact while conducting an operational deployment. Like the Army Protection Program, it focuses on Army leadership, protection responsibilities, and mission accomplishment. Deploying commanders in a contested environment have the added task of safeguarding their forces. They must think and act as if in an operational environment, outside the United States, facing the enemy in an unfamiliar domain. The concepts universally apply, whether in a threatened homeland or in Iraq or Afghanistan. Army Doctrine Publication 3-37 states, “The

22. HQDA, *Army Protection Program*, 35.

23. Fort Hood Army Internal Review Team, *Final Report*, 3, 13, 19–20.

24. HQDA, *Army Protection Program*.

25. HQDA, *Protection*.

commander's inherent responsibility to protect and preserve the force and secure the area of operations (AO) is vital in seizing, retaining, and exploiting the initiative."²⁶

The wars and operating environments of the future will require a change in mindset. The assumption the area from which a deployment initiates is a safe zone must change. The area must be regarded as an operational area with an active threat to the deploying force's operation. Applying Army Doctrine Publication 3-37 to this scenario, "Protection must be considered continuously throughout the operations process to identify threats and hazards; implement control measures to prevent or mitigate enemy or adversary actions; and manage capabilities to mitigate the effects and preserve time to react or maneuver against the enemy to gain superiority and retain the initiative."²⁷

The bottom line—deployments from home will have to be executed under new rules in future war scenarios, and the Army must provide actively for its protection or be wiped out before ever getting "over there."²⁸ These protection functions entail "[a]ctive defensive measures to protect friendly forces, civilians, and infrastructure" from an enemy or adversary.²⁹ Besides the deployment effort, the deploying force's workload will include the protection tasks in the doctrine that are of particular importance to a deployment. These tasks are operations security, intelligence and antiterrorism operations, survivability operations, force health protection, and personnel recovery operations.³⁰

The physical merger between deploying and garrison forces should coincide at the Protection Executive Committee. The committee "is the APP management structure at commands, installations, and stand-alone facilities that leverages APP principles and best practices to coordinate, integrate, synchronize, and prioritize resources with a unity of effort across the APP functional elements of protection."³¹ The deploying commander should therefore establish a protection cell and protection working group per the doctrine and colocate them with the installation Protection Executive Committee.³² These planning and execution cells serve similar functions and can jointly address issues. The Protection Executive Committee, in conjunction with the working groups, develops integrated protection plans that detail critical base and continuity operations that must be protected.³³

The installation's emergency operations center provides "information management, resource management, coordination, and emergency communications" during emergencies or events that could "impact the installation's mission, personnel, and/or

26. HQDA, *Protection*, 1-3.

27. HQDA, *Protection*, 1-3.

28. Tussing and Parker, "Multi-Domain Battle."

29. HQDA, *Protection*, iv.

30. HQDA, *Protection*, 1-5-1-6.

31. HQDA, *Army Protection Program*, 8.

32. HQDA, *Protection*.

33. HQDA, *Army Protection Program*, 11.

infrastructure.”³⁴ In a contested deployment, the emergency operations center would serve as the focal point for activities between deploying forces and the garrison. Manned with garrison staff and the deploying unit’s protection cell and protection working group representatives, the center could oversee and coordinate activities throughout the deployment. As the installation command, deploying unit, and local authorities establish a movement corridor for the deploying elements—that is, a “designated area established to protect and enable ground movement along a route”—the center would monitor movement and security.³⁵ Its activities among the garrison, deploying units, local civil authorities, and higher and adjacent elements would provide a coordinated approach to protection.

Ultimately, the Army relies on critical, external enablers to deploy. Agencies and commands within the Department of Defense (most notably, US Transportation Command) and federal, state, and local authorities whose domains the Army must move on and through are essential partners. Along with roads, rail lines, embarkation ports, and airfields located in the civil sector, the Army uses contracted commercial sources. Coordination between the Army and civil entities is largely logistical. In a contested environment, this coordination must also focus on protection. Services and support for movement must be safeguarded, and, sometimes, one of these services must be protection itself.

A changing operational mindset can leverage the strong ties the Army enjoys with American society to support the Army in a contested homeland. An Army post and the families it houses are part of the fabric of the communities in which they are located. As an enterprise, the Army is financially important to its off-post neighbors. The relationship goes beyond routine, mutual cooperation and economic benefits; it extends to emergency response, support during crises, and the shared experience of pulling together during tough times. The *Fort Hood Army Internal Review Team: Final Report* highlights and reinforces these relationships serve both the Army’s and the community’s interests.³⁶ The Army Protection Program stresses Army installations must establish agreements with civil officials for critical response and support to benefit both the Army and the community.³⁷ For example, in December 2017, the Madigan Army Medical Center at Joint Base Lewis-McChord received and treated injured passengers from an Amtrak derailment in nearby Tacoma, Washington.³⁸ This incident is one of many that demonstrate how military communities interact with civil components in a beneficial

34. HQDA, *Army Emergency Management Program*, Army Regulation 525-27 (Washington, DC: HQDA, March 29, 2019).

35. HQDA, *Protection*, 2-11.

36. Fort Hood Army Internal Review Team, *Final Report*, 4-5.

37. HQDA, *Army Protection Program*.

38. KOMO Staff, “Hospitals: Most Injured Victims of Derailment in Improving Condition,” KOMO News, December 19, 2017, <https://komonews.com/news/local/hospitals-report-most-injured-victims-of-amtrak-derailment-improving>.

and synergistic way to provide critical services and resiliency. “The strength of our nation is our Army,” and the strength of our Army is our nation.³⁹

The strong, supportive relationship between military and civil elements must be harnessed if the United States is to survive future war in the homeland, and these bonds must be leveraged in a contested deployment. Civilian law enforcement and Army protection officials must coordinate in detail – and in advance – to ensure soldiers can operate and deploy in a contested environment. Proactive information sharing is vital to both the Army and civil elements. During this cooperation, the Army may be able to offer safety and security support to the local population.

Local authorities who agree to provide support to the Army may need to reach up their chains of command and out to their support networks for backup in contested deployment scenarios. Likewise, the Army must share information on civil-military support agreements up the APP chain of command for awareness and integration at the national response level. The APP provisions and structure are the chain of command for this type of coordination. Per the Army Protection Program, the Department of the Army maintains management and oversight boards and planning and assessment documents and communicates throughout the service and outward to the Office of the Secretary of Defense, other services, and federal agencies.⁴⁰ The purpose of these activities is to coordinate and integrate the protection of the Army with the Joint Force and interagency and intergovernmental organizations.⁴¹ Local coordination for protection is a necessary and logical first step between bases and local officials. Ultimately, the communication of protection needs in a contested environment must be formalized at the national level.

The *US Army Operating Concept* indicates the Army must be “ready to protect the American people and respond to crises in the homeland.”⁴² One of the Army’s missions is to support civil authorities in securing the homeland, also known as Defense Support to Civil Authorities (DSCA).⁴³ In a contested deployment, however, the traditional defense support of civil authorities paradigm would likely change radically. If a military deployment becomes one of the nation’s main efforts, then support tasks arising from the Department of Homeland Security *National Preparedness Goal* would likely take a back seat.⁴⁴ The foundation and principles of the *National Preparedness Goal*, as laid out in Presidential Policy Directive 8 and its

39. Ash Carter, “Army Chief of Staff Change of Responsibility” (speech, Fort Myer, VA, August 14, 2015), <https://www.defense.gov/Newsroom/Speeches/Speech/Article/613676/army-chief-of-staff-change-of-responsibility/>.

40. HQDA, *Army Protection Program*, 8–10.

41. HQDA, *Army Protection Program*, 8–10.

42. TRADOC, *US Army Operating Concept*, 17.

43. William J. Lynn III, *Defense Support of Civil Authorities*, Department of Defense Directive 3025.18 (Washington, DC: Under Secretary of Defense for Policy, updated March 19, 2018).

44. Department of Homeland Security (DHS), *The National Preparedness Goal*, 2nd ed. (Washington, DC: DHS, September 2015).

supporting National Preparedness System (NPS), provide the fundamental way ahead for exploring a framework for support and response to the military as a priority.⁴⁵

Although the NPS doctrine and related processes typically operate in a permissive environment in which defense supports civil authorities, the doctrine does not preclude civil authorities from supporting defense in a contested deployment. The National Preparedness System envisions a wide range of scenarios, and the process that facilitates the planning and execution of this mission is the National Response Framework (NRF), which is “built on scalable, flexible, and adaptable concepts identified in the National Incident Management System.”⁴⁶ The framework “is a guide to how the Nation responds to all types of disasters and emergencies,” and the National Incident Management System, which supports the National Response Framework, “provides a common, interoperable approach to sharing resources, coordinating and managing incidents, and communicating information.”⁴⁷ Together, they “provide a single, comprehensive, nationwide approach to incident management.”⁴⁸

The National Response Framework is the recognized structure and process used by the United States to plan national responses to natural or man-made challenges, emergencies, and crises. It provides a flexible and capable framework for facilitating planning, determining requirements, and assigning response forces for scenarios in which the Army might be designated the national priority.⁴⁹ Such scenarios would require a change in mindset to the ways the framework has operated in past. In this scenario, the Army would be the supported unit rather than the supporting unit.

The framework is a good starting point for planning support to a contested deployment of Army forces. If the top emergent priority for the United States is deploying the Army in a contested homeland, then the requirements for mobilization, movement, protection, and embarkation would be the focus of the framework. The Department of Homeland Security would oversee “preparedness activities within the United States to respond to and recover from terrorist attacks, major disasters, and other emergencies.”⁵⁰ The department has the authorities, structure, processes, and oversight of the National Response Framework. The Army’s and the nation’s first option in dealing with a contested homeland, notwithstanding the need for adaptation, should be tried-and-true concepts and doctrine for homeland security. Understanding this new and different battlespace and the rules governing it is essential for the military to ensure its requirements are identified.

45. Barack Obama, *National Preparedness*, Presidential Policy Directive 8 (Washington, DC: White House, March 30, 2011).

46. DHS, *National Response Framework*, 4th ed. (Washington, DC: DHS, October 28, 2019), i.

47. US Army War College (USAWC), *How the Army Runs 2019–2020: A Senior Leader Reference Handbook* (Carlisle, PA: US Army War College Press, 2020), 20-4; and Federal Emergency Management Agency (FEMA), “NIMS Components—Guidance and Tools,” FEMA, updated February 18, 2021, <https://www.fema.gov/emergency-managers/nims/components>.

48. USAWC, *How the Army Runs*.

49. DHS, *National Response Framework*.

50. DHS, *National Response Framework*, 34.

Both civil and military authorities, led by the Department of Homeland Security and the Department of Defense, would need to converge on this problem set with the National Response Framework as the focal point, share situational awareness, and envision how they will work together in an operating environment in which the military may be at war in the homeland as it deploys.

Although the Department of Homeland Security oversees the security of the United States and its citizens in this complex endeavor, it relies on, and must be supported by, numerous partners and stakeholders.⁵¹ The concepts of resilience and coordinated response to hazards and emergencies represent a whole-of-government and whole-of-nation approach. The basic precept of the National Preparedness System is a tiered, bottom-up approach to supporting and responding.⁵² The Army's role in this process is to provide for its internal protection as much as possible and to identify its requirements in detail to the Department of Homeland Security. To be most effective, the National Preparedness System recognizes communities should conduct their own risk- and capability-based planning that will help them identify capability gaps—planning that should also be done at the unit level.⁵³

One of the five mission preparedness areas is protection “to achieve the goal of a ‘secure and resilient nation.’”⁵⁴ The result of local or unit-level assessment of capabilities is the determination of the support and response that can be provided.⁵⁵ The Army must determine its requirements, the areas it can support for itself, and its shortfalls in protecting its deployment operation. The coordination of this information and the entities that provide it are placed within the “unity of effort through unified command” principle in the response mission area.⁵⁶ In addition, 15 response or core capabilities (also referred to as emergency support functions) address protection and other requirements of a deploying force.⁵⁷ Functions of particular importance are information and planning, transportation, cross-sector business and infrastructure, public safety and security, and public health and medical services.⁵⁸

The formulation process for mapping out support and response capabilities is adaptable to the protection required for a deploying Army. The process, supported by a coordination system known as the National Incident Management System, includes the institutionalized and accepted framework for planning and executing domestic security and hazard response.⁵⁹ This system provides “for standardized but flexible incident management and support practices that emphasize common principles, a consistent

51. DHS, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: DHS, June 18, 2014).

52. DHS, *National Response Framework*, 6–7.

53. DHS, *National Response Framework*, 47.

54. DHS, *National Response Framework*, 12.

55. DHS, *National Response Framework*, 48.

56. DHS, *National Response Framework*, 7.

57. DHS, *National Response Framework*.

58. DHS, *National Response Framework*, 21–22.

59. DHS, *National Response Framework*, ii.

approach for operational structures and supporting mechanisms, and an integrated approach to resource management.”⁶⁰

Given this construct, the Army and the Department of Defense writ large must evaluate the scenarios within a contested homeland where they will require support and response for their deployment and the security of their bases. The Army is operating on the Department of Homeland Security’s turf and must confirm how its protection needs will be met. The military must identify its requirements and determine how it will receive support. The tiered, bottom-up approach to planning in the National Response Framework normally focuses on the capabilities providers possess in anticipation of the responses that will likely be required. The Army must predetermine its requirements and set conditions within the framework for the support it will need from civil elements. Identification and visibility of Army requirements will allow for planning and matching up of national capabilities for support. The Army can and should initiate the coordination for this support with local and state officials while adhering to the bottom-up construct. Agreements established between base commanders and local police, sheriffs, and state law enforcement organizations using the APP process for dialogue and coordination are an effective means of coordinating support. Final adjudication and approval of these arrangements must be done by the Departments of Defense and Homeland Security. Oversight of this plan will be done by the Department of Homeland Security, since it is responsible for the National Response Framework.

Once solutions to Army protection shortfalls and other deployment requirements have been determined, they should be codified in the National Response Framework. This type of agreed-upon support, whether determined locally or at higher levels within the National Preparedness System, could be further classified as prescribed mission assignments at the federal level among government partners.⁶¹ At the local or state level, agreed-upon support would be predetermined similarly using memoranda of agreement. An example of such an agreement for support is local law enforcement reinforcing the base perimeter or providing additional gate security. The base’s requirements and local law enforcement’s capabilities, once negotiated and agreed upon, would be formalized like prescribed mission assignments for ease and speed of execution. Ultimately, the National Resposne Framework would become the final repository for requirements and for the identification of the entities providing response to the Army.

Many other options for support to Army deployment requirements could develop within this construct. For example, Army or DoD assets could be resourced for critical protection functions as part of this deliberation. Active units not in deployment mode could backfill shortfalls or reinforce installation functions within the Army Protection Program. These units could be tasked by the Army to alleviate burdens on deploying units for route security when transporting sensitive or high-value items in convoys or at assembly areas awaiting movement. This task could even involve other services or force providers. The bigger picture, however, is the NPS methodology is the recognized process for planning for solutions in a contested deployment environment. Bottom-up

60. DHS, *National Response Framework*, 11.

61. FEMA Emergency Management Institute, *IS-75: Military Resources in Emergency Management* (Washington, DC: FEMA, May 2011).

planning conducted within Army and DoD prerogatives and authorities is the first step, but plugging into the National Response Framework with clear requirements and prescribed support will be essential to ensure civil assistance.

Civil and military relations in a contested homeland is a new chapter in warfare for the United States and its armed forces. Contested deployment embodies a hybrid state of warfare the United States has not encountered before. Active-duty Army operations in the homeland and aggression by an enemy in which facilities, families, and units are engaged constitute an unfamiliar scenario for the United States, at least in modern times. As a nation and Army, we must assess this new threat and formulate a response to it in advance. Dealing with the next generation of enemy tactics or weapons, especially if they will be used within US borders, will be a huge challenge. What we must not do is make this challenge harder than necessary. The United States has the doctrine to provide for the Army's protection in a contested homeland. Adapting the United States' mindset to a new form of conflict and harnessing the collective strength of the nation will place the country ahead of the next incident or attack and allow the Army to continue its mission.

The Army's ability to defend the nation beyond its borders is enabled by the country's capabilities "to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation."⁶² The novel situation of contested deployment will require the Army and homeland security agencies to develop a different warfare perspective. Adaptation, planning, and exercising this concept will provide resilience and response for protecting the Army and its ways and means when it is deploying in a high-threat environment.

The way forward is to begin soon to identify national priorities within the National Response Framework related to Army deploying forces—protection of the forces being a chief priority—and ensuring Army requests for assistance are addressed in advance. The framework is specifically designed for this preplanning, and its response areas should deliver the support required. The appropriate solution, provider, or partner must be identified at the local, county, state, or federal level to meet the protection requirements for the Army. Safe access to roads, bridges, marshaling areas, refueling and rest stops, ports, and airfields and the ability to access common-use architecture (such as cell-phone towers and the Internet) must be provided through the National Response Framework.

The doctrine for military and civil cooperation in national emergencies must evolve to identify a contested homeland where the military needs civil support operations. With this scenario written into the doctrine for greater clarity, and with coordination between DoD and DHS partners, the challenge of projecting forces under duress can be successfully met. Building national resilience to support the Army's deployment requirements within a contested homeland is a compelling readiness issue. The United States must be ready now (the threat is real and on US soil), and the nation must be ready for what is next (anticipating new threats and continuing to evolve Army, DoD, and DHS doctrine). New solutions with a whole-of-nation approach to war will ensure the homeland is secure so it can be defended.

62. Obama, *National Preparedness*.

3. STRATEGIC SEAPORTS AND NATIONAL DEFENSE

The United States is dependent upon its seaports to project military power around the world. In a major conflict, 90 percent of US military cargo would ship by sea.¹ Today's military port infrastructure is concentrated in 22 strategic seaports.² Seventeen of the strategic seaports are commercial ports where the Department of Defense (DoD) ships its equipment, in the event of military conflicts overseas, alongside civilian commercial shipments.³ These strategic seaports have effectively supported the Afghanistan War, the Iraq War, and US involvement in the Syrian Civil War over the last 20 years, but the ports may be insufficient to support the next war.

In his *Summary of the 2018 National Defense Strategy of the United States*, Secretary of Defense James Mattis made clear his concerns about US infrastructure in the next conflict.

It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.⁴

Clearly, the American security environment has changed. The United States' dependence on its strategic seaports to project power makes these seaports a likely target in a future conflict.

In World War II, the American military mobilized and deployed its forces from the uncontested and relatively safe continental United States (CONUS). The United States had a strong industrial base supported by a robust and modern transportation infrastructure. The US economy was totally mobilized and coordinated by government for war.⁵ The American people were united after 1941 to work and sacrifice to support the war effort against the Axis powers, and 97 percent of Americans supported going to war with Japan after the Pearl Harbor attack.⁶

1. Zina D. Merritt, *Defense Logistics: The Department of Defense's Report on Strategic Seaports Addressed All Congressionally Directed Elements*, GAO-13-511R (Washington, DC: Government Accountability Office, May 13, 2013), 1.

2. Merritt, *Defense Logistics*, 7.

3. Merritt, *Defense Logistics*, 1.

4. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: Department of Defense, January 2018), 3.

5. Doris Goodwin, "The Way We Won: America's Economic Breakthrough during World War II," *American Prospect*, December 19, 2001, <https://prospect.org/health/way-won-america-s-economic-breakthrough-world-war-ii/>.

6. David W. Moore, "Support for War on Terrorism Rivals Support for WWII," Gallup (website), October 3, 2001, <https://news.gallup.com/poll/4954/support-war-terrorism-rivals-support-wwii.aspx>.

Today, much of the US transportation infrastructure is so old and in need of repair the American Society of Civil Engineers published *Failure to Act* in 2013 to show investment shortfalls in US infrastructure.⁷ The Department of Defense must consider the current state of US port infrastructure when planning for future wars. This chapter explores the current state of US strategic seaports by focusing on the condition of the ports, the criteria used to select strategic seaports, and federal government efforts to maintain port readiness. Further, the chapter will review the emerging threats to mobilization at strategic seaports and offer recommendations to improve the system.

Strategic seaports are designated by the commanding general of Military Surface Deployment and Distribution Command (SDDC), which is the US Army component of United States Transportation Command.⁸ Today, 22 ports are included in the Strategic Seaport Program.⁹ The Department of Transportation Maritime Administration, in partnership with Military Surface Deployment and Distribution Command, manages the Strategic Seaport Program for the Department of Defense.¹⁰ The Maritime Administration chairs the National Port Readiness Network.¹¹ Nine federal agencies are members of the network: the Maritime Administration, the US Army Corps of Engineers, the Military Surface Deployment and Distribution Command, the US Coast Guard, Military Sealift Command, US Army Forces Command, the Transportation Security Administration, US Northern Command, and US Transportation Command.¹²

Civilian ports work with Military Surface Deployment and Distribution Command to become strategic seaports. This relationship brings revenue to the port and the communities in which they are located; business at the port means work for equipment operators, truck drivers, and stevedores.¹³ These facilities are selected to be strategic seaports based on criteria such as proximity to highways, rail access, and the number and length of ship berthing spaces.¹⁴

A study conducted for Military Surface Deployment and Distribution Command in 2008 assessed the viability of strategic seaports in a future conflict and serves as a basis

7. American Society of Civil Engineers, *Failure to Act: Closing the Infrastructure Investment Gap for America's Future* (Reston, VA: American Society of Civil Engineers, 2013).

8. "Strategic Seaport Program," US Army, February 28, 2017, https://www.army.mil/standto/archive_2017-02-28.

9. Merritt, *Defense Logistics*, 7.

10. Merritt, *Defense Logistics*, 9.

11. Merritt, *Defense Logistics*, 9.

12. "National Port Readiness Network (NPRN)," Department of Transportation Maritime Administration, updated December 8, 2020, <https://www.maritime.dot.gov/ports/strong-ports/national-port-readiness-network-nprn>.

13. "Gulfport Achieves Strategic Seaport Designation," WLOX, November 19, 2015, <https://www.wlox.com/story/30562438/gulfport-achieves-strategic-seaport-designation>.

14. David McClean, "SDDC Port Look Study 2008" (PowerPoint presentation, Strategic Ports Workshop, American Association of Port Authorities, March 23, 2009), <https://aapa.files.cms-plus.com/SeminarPresentations/2009Seminars/09OpsSafetyIT/Jungwaelter.pdf>.

of a way forward for the command in the selection of ports, the number of ports required for the Department of Defense, and the manning of the ports by DoD personnel.¹⁵ The study, entitled *Port Look 2008*, examined three scenarios using a force-sizing construct from the 2006 Quadrennial Defense Review.¹⁶ The study focused on a homeland defense surge, a war on terror/irregular warfare surge, and a conventional campaign.¹⁷ Further, the study predicted a maximum daily cumulative throughput for ports on the East Coast, Gulf Coast, West Coast, and the Alaskan coast for the year 2015.¹⁸ The study concluded the strategic seaports on the Alaskan coast and the Gulf Coast had minor shortfalls in throughput capacity, but they could be compensated for easily with the addition of alternate ports.¹⁹

The 2012 National Defense Authorization Act directed another study of strategic seaports to be performed; this report served as a follow-up to *Port Look 2008*.²⁰ The Government Accountability Office (GAO) reviewed the findings of the report in 2013. The GAO report centered on four areas: the structural integrity of strategic seaports, the impact on operational readiness if recommended improvements were not made, potential funding sources if improvements were not made, and whether the Department of Defense had sufficient authority to direct the improvements.²¹

The 22 strategic seaports had some structural deficiencies. Fifteen ports had minor deficiencies with negligible impact. Four ports had deficiencies with minor impact. One port had significant deficiencies that impaired its ability to support its mission. Two ports had major deficiencies that resulted in major obstacles to deployment.²² The deficiencies ranged from poor facilities maintenance to the need for entire wharves to be replaced.²³ In its report, the Government Accountability Office concluded the listed deficiencies had been addressed; however, the exact nature of the deficiencies and the solutions to them were not listed in the unclassified version of the report. In addition, the criteria used to assess the seaports were not specified.

An example of a port in need of structural improvement is the Port of Alaska, the closest strategic seaport to Fort Wainwright.²⁴ News reports from late 2017 revealed the port had serious structural problems. Many of the pier pilings were made from pipe

15. Military Surface Deployment and Distribution Command (SDDC), *Port Look 2008: Strategic Seaports Implementation Plan* (Scott Air Force Base, IL: SDDC, October 2008).

16. Donna J. Simkins et al., *Port Look 2008: Strategic Seaports*, Report SDD80T1 (Tysons, VA: LMI Government Consulting, October 2008).

17. Simkins et al., *Port Look 2008*.

18. Simkins et al., *Port Look 2008*, 1:3-7.

19. Simkins et al., *Port Look 2008*, 1:6-1-6-2.

20. Merritt, *Defense Logistics*.

21. Merritt, *Defense Logistics*, 2.

22. Merritt, *Defense Logistics*, 15.

23. Merritt, *Defense Logistics*, 16.

24. Municipality of Anchorage, *2020 Approved Utility/Enterprise Activities Budgets* (Anchorage, AK: Municipality of Anchorage, October 2, 2019).

left over from the construction of the Trans-Alaska Pipeline.²⁵ The saltwater had taken its toll, and many of the pilings had corroded.²⁶ In June 2017, some of the pilings gave way while a large Holland America cruise ship was docking, and a portion of the pier broke away and sank into the water. The ship was not damaged, but the incident illustrates the potential consequences of structural deficiencies.²⁷

The Port of Alaska has other structural problems as well. A 2003 expansion project was halted in 2010 when damage was discovered in the support structures designed to support the new dock. This halting of operations cost state, local, and federal taxpayers \$300 million.²⁸

The Port of Alaska is a critical port for the state—90 percent of the freight traffic in Alaska comes in by sea, and half of this traffic stops at the port.²⁹ The port is critical to the deployment and sustainment of Alaska's military bases and is the key port for disaster relief.³⁰ Alaska experiences frequent earthquakes, and, in the event of a severe earthquake, such as the one that occurred in 1964, the Port of Alaska would be critical to recovery efforts and defense support of civil authorities.³¹

To gain a clear understanding of the findings of the two reports and determine whether their findings hold true, one must look at the criteria used. The 2008 report was working under the assumptions of the 2006 Quadrennial Defense Review. Written under the tenure of Secretary of Defense Donald Rumsfeld, a member of the George W. Bush administration, the *Quadrennial Defense Review Report* paints a picture of a different world than the one we live in today.³² The report talks about the military moving “[f]rom major conventional combat operations—to multiple irregular, asymmetric operations.”³³ The document only mentions Korea four times in 113 pages.³⁴ Russia is described as a “country in transition” that is “unlikely to pose a military threat to the United States or its allies.”³⁵ China, the report says, has the potential to compete militarily with the United States because China had been investing in its military since

25. Elwood Brehmer, “Anchorage Port Gets New Name, but Problems Remain,” AP News (website), November 18, 2017, <https://apnews.com/article/10265c71e3dc4cc5a96b95421d0a7ae1>.

26. Brehmer, “Anchorage Port Gets New Name.”

27. Devin Kelly, “Anchorage’s Port Is Already Falling Apart. With the Clock Ticking, Who Will Pay to Fix It?,” *Anchorage Daily News*, August 14, 2017, <https://www.adn.com/alaska-news/anchorage/2017/08/14/anchorages-port-is-already-falling-apart-with-the-clock-ticking-whats-the-plan/>.

28. Brehmer, “Anchorage Port Gets New Name.”

29. Brehmer, “Anchorage Port Gets New Name.”

30. Brehmer, “Anchorage Port Gets New Name.”

31. “The Great M9.2 Alaska Earthquake and Tsunami of March 27, 1964,” US Geological Survey Earthquake Hazards Program, n.d., <https://earthquake.usgs.gov/earthquakes/events/alaska1964/>.

32. Office of the Secretary of Defense (OSD), *Quadrennial Defense Review Report* (Washington, DC: OSD, February 6, 2006).

33. OSD, *Quadrennial Defense Review Report*, vii.

34. OSD, *Quadrennial Defense Review Report*.

35. OSD, *Quadrennial Defense Review Report*, 28–29.

the 1990s; however, the US policy was to encourage China to be “an economic partner and emerge as a responsible stakeholder and force for good in the world.”³⁶

In his *2018 National Defense Strategy Summary*, Secretary Mattis states threats to the United States have changed: “Inter-state strategic competition, not terrorism, is now the primary concern in US national security.”³⁷ China, Russia, North Korea, and Iran posed significant threats to the United States in a way they were not thought to in the past, and terrorists and transnational criminal organizations were still a threat.³⁸

Since the terrorist attacks of 9/11, the US government has placed significant emphasis on security at US ports.³⁹ In 2006, Congress passed the Security and Accountability for Every Port Act to address port security.⁴⁰ The act addressed the threat of a terrorist attack on a seaport, and great strides were made in strengthening the physical security of seaports.⁴¹ Following this legislation, “[t]he Port Security Grant Program has helped develop and sustain prevention, preparedness, and response capabilities around ports.”⁴²

When Military Surface Deployment and Distribution Command surveys strategic seaports, the criteria it uses to determine their viability for military use does not take the current operating environment into account. *Port Look 2008* used the following criteria to evaluate strategic seaports: facilities (access and capabilities), attitude (stakeholder perspective), availability, price (cost for terminal operation and workforce), background (history of use by the military), location (proximity to DoD shippers), and resources (personnel).⁴³ This criteria does not take into account the multi-domain threats the US military would face in the event of mobilization in a contested environment.

How does the new operational environment impact US strategic seaports? The old criteria addressed physical security, but did not take into account the kind of threats former Secretary Mattis referred to in the *2018 National Defense Strategy*. Cyberwarfare is an easy-entry, low-cost way to disrupt the US military’s movement through its strategic seaports.

In a 2013 Brookings Institution policy paper, US Coast Guard Commander Joseph Kramek raised concern about the threat of cyberattacks on some of the largest ports in the United States. According to Kramek, “unlike other sectors of critical infrastructure,

36. OSD, *Quadrennial Defense Review Report*, 29.

37. Mattis, *Summary of 2018 National Defense Strategy*, 1.

38. Mattis, *Summary of 2018 National Defense Strategy*, 3.

39. John D. Donahue and Mark H. Moore, eds., *Ports in a Storm: Public Management in a Turbulent World* (Washington, DC: Brookings Institution Press, 2012), 15.

40. Henry W. Willis, “Ten Years after the Safe Port Act, Are America’s Ports Secure?,” *RAND Blog*, April 6, 2016, <https://www.rand.org/blog/2016/04/attractive-targets.html>.

41. *Evaluating Port Security: Progress Made and Challenges Ahead*, 113th Cong. (2014) (statement of Stephen L. Caldwell, Director, Homeland Security and Justice, Government Accountability Office).

42. Willis, “Ten Years After.”

43. Simkins et al., *Port Look 2008*, 1:2-1-2-2.

little attention has been paid to the networked systems that undergird port operations.”⁴⁴ This vulnerability is a consequence of the linked systems that make the ports efficient and profitable.

A network of complex systems manages large, modern ports today. Cranes and container-handling equipment use optical technology to read barcodes and radio frequency identification interrogators to locate freight. Computer systems provide instructions to automated equipment to move and organize containers around the port. For example, the Port of Long Beach, which is a strategic seaport, uses “robots, artificial intelligence, and other digital tools to choreograph the complicated dance that keeps goods flowing.”⁴⁵

Linked automation systems are vulnerable, and adversaries are aware of the vulnerability. The cybersecurity company TrapX discovered the “Zombie Zero” attack method in 2014. TrapX states in a white paper it “believe[s] that the Zombie Zero malware was preloaded into newly manufactured scanners by a manufacturer in China.”⁴⁶ The targeted company had 16 infected scanners, which allowed the malware to probe the network and identify specific servers, granting the hackers complete access to the company’s data.⁴⁷ Both the manufacturer and the hackers are believed to be linked to the Chinese government.⁴⁸

A more recent example of a cyberattack on a US port occurred in June 2017 at the Port of Los Angeles. The attack came in the form of the malware “NotPetya,” which ravaged Ukraine’s power system and government computer systems the same year. The malware spread to millions of computers in several countries in a matter of hours. When NotPetya hit the Maersk terminal in the Port of Los Angeles, it shut down operations and affected 17 other Maersk terminals around the world.⁴⁹ Congresswoman Norma Torres of California, who proposed a bill in Congress to address port cybersecurity, said, “The most recent cyber-attack revealed serious vulnerabilities in our nation’s maritime security.”⁵⁰ Clearly, this cyberattack was very destructive; it spread very quickly and affected systems all over the world.

Another way ports could be affected by a cyberattack is through the Global Positioning System (GPS) signals container-moving equipment uses to locate containers and move

44. Joseph Kramek, *The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities* (Washington, DC: Brookings Institution Press, July 2013).

45. Clay Dillow and Brooks Rainwater, “US Ports Take Baby Steps in Automation as Rest of the World Sprints,” *Fortune*, January 30, 2018, <https://fortune.com/2018/01/30/port-automation-robots-container-ships/>.

46. TrapX Research Labs, *Anatomy of an Attack – Zombie Zero; Weaponized Malware Targets ERP Systems* (Waltham, MA: TrapX Security, March 1, 2017), 5.

47. TrapX Research Labs, *Anatomy of an Attack*, 8.

48. TrapX Research Labs, *Anatomy of an Attack*, 5.

49. Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017, H.R. 3101, 115th Cong. (2017).

50. Strengthening Cybersecurity Information Sharing.

them around ports.⁵¹ In a report by the cybersecurity company CyberKeel of Denmark, maritime cyber expert Lars Jensen states, “Powerful GPS jammers are readily available on the commercial market—whilst this is not legal everywhere, the fact remains that they are easy to obtain.”⁵² In a 2014 incident at a US port, a seven-hour GPS disruption brought the port to a standstill.⁵³ Although these incidents would not cripple a military deployment by themselves, US ports are clearly not safe from cyberattacks.

The use of GPS by much of the transportation industry also makes the technology a major vulnerability. Cranes use GPS to locate containers and move them around ports. Ships use GPS for navigation. A maritime navigation expert said in a recent article GPS is “a free, highly precise signal that engineers have incorporated into virtually every technology. But because of that, it’s become a single point of failure for much of America.”⁵⁴

The Coast Guard is the lead agency for port security. But the Government Accountability Office found in 2014 the actions taken by the service to assess cyber risk in US ports were insufficient. The Coast Guard’s legally mandated maritime security plans did not identify or address cybersecurity threats, and the mechanisms used to coordinate with other maritime stakeholders were not sufficient.⁵⁵ The office recommended the Department of Homeland Security “direct the Coast Guard to (1) assess cyber-related risks, (2) use this assessment to inform maritime security guidance, and (3) determine whether the sector coordinating council should be reestablished.”⁵⁶

In June 2015, the Coast Guard released the *United States Coast Guard Cyber Strategy*, in which the service articulated its vision to “ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation’s critical maritime infrastructure.” The service also states the “maritime critical infrastructure and the [Maritime Transportation System] are vital to our economy, national security, and national defense.”⁵⁷ Further, to achieve its mission of protecting maritime infrastructure, the Coast Guard will focus on working with the Department of Homeland Security (DHS) and coordinating with the owner-operators of the Maritime

51. Lily Hay Newman, “What If a Cybersecurity Attack Shut Down Our Ports,” *Slate*, May 11, 2014, https://www.slate.com/articles/technology/future_tense/2015/05/maritime_cybersecurity_ports_are_unsecured.html.

52. CyberKeel, *Maritime Cyber-Risks* (Copenhagen: CyberKeel, October 15, 2014), 12.

53. Newman, “What If.”

54. Newman, “What If.”

55. Gregory C. Wilshusen and Stephen L. Caldwell, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, GAO-14-459 (Washington, DC: Government Accountability Office, June 2014), 2.

56. Wilshusen and Caldwell, *Maritime Critical Infrastructure Protection*, 2.

57. US Coast Guard (USCG), *United States Coast Guard Cyber Strategy* (Washington, DC: USCG, June 2015), 10, 12.

Transportation System to “improve cybersecurity information sharing and develop and implement risk-based standards.”⁵⁸

Whether the Coast Guard’s efforts to emphasize cybersecurity at US ports are improving their cyber defense posture is unclear, but some improvements have been made. The service’s *Port Operations Handbook 2015 Edition* includes a portion on cyber risk management for port operators and provides tips for safeguarding the Maritime Transportation System from cyberattack. The handbook offers links to four websites port operators can visit for further information from the Coast Guard and other US government agencies.⁵⁹ The handbook and the strategy have progressed, but still do not go far enough.

In 2016, the Government Accountability Office again examined critical transportation infrastructure in two reports. The first report called for the Department of Homeland Security to develop metrics for assessing the effectiveness of voluntary cybersecurity standards, and the second report noted the DHS cyber risk mitigation efforts were still deficient in some areas.⁶⁰ In addition, the office found some issues were still unresolved in a February 2018 report.⁶¹ The department noted in an addendum to the report the voluntary nature of the programs “hamper efforts to adopt the framework,” and the Department of Homeland Security would continue to work with its partners to support the adoption of the program.⁶² This information indicates the US government is focused on protecting US critical infrastructure from cyberattack. Improvements, however, should still be made. Perhaps more incentives for owner-operators of US ports to shore up their cyber defenses would help to realize these improvements.

To illustrate the military’s degree of dependence on strategic seaports, a cyberattack on the Port of Beaumont “would impact almost 50 percent of all military cargo bound for overseas contingency operations.”⁶³ Further, an adversary gaining access to the Army logistics management system network would impact the transportation of military cargo worldwide.⁶⁴

Though the Army uses robust cybersecurity measures in its terminal operations, commercial systems are still vulnerable. In 2012, a foreign military infiltrated multiple systems aboard a commercial ship contracted by US Transportation Command.⁶⁵ The

58. USCG, *Coast Guard Cyber Strategy*, 31.

59. USCG, *Port Operators Handbook 2015 Edition* (Washington, DC: USCG, 2015), 154.

60. Gregory C. Wilshusen, *Measures Needed to Assess Agencies’ Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, DC: Government Accountability Office, December 2015); and Gregory C. Wilshusen, *Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, DC: Government Accountability Office, November 2015).

61. Nick Marinos, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, Government Accountability Office-18-211 (Washington, DC: Government Accountability Office, February 2018).

62. Marinos, *Critical Infrastructure Protection*, 38.

63. Kramek, *Critical Infrastructure Gap*.

64. Kramek, *Critical Infrastructure Gap*, 23.

65. USCG, *Coast Guard Cyber Strategy*, 12.

weakness was not in the military systems, but in the commercial system that carried information about military shipments on commercial vessels. Clearly, progress still needs to be made to secure US ports and shipping companies from cyber threats.

Other types of threats to strategic ports exist as well. The proliferation of weapons capable of creating an electromagnetic pulse (EMP) places both US ports and the US way of life in jeopardy. Congress created a commission in October 2000 to assess the threat of an EMP attack and propose ways to defend against it.⁶⁶ In 2004 and 2008, the commission stated, “99% of the US Military is dependent on the civilian electric grid.”⁶⁷ In 2004, in a congressional hearing on the threat of EMP weapons, the EMP Commission reported, “[T]he knowledge and technology to develop super-EMP weapons had been transformed to North Korea and that North Korea could probably develop these weapons in the near future.”⁶⁸ If an EMP weapon were detonated 250 miles (400 kilometers) over the United States, the detonation would affect the entire country; at a lower altitude, it would affect a smaller portion of the country.⁶⁹ The commission was disbanded on September 30, 2017, and no significant action has been taken to mitigate the threat.⁷⁰

In a speech to the Air Force Association Air, Space, and Cyber Conference in National Harbor, Maryland, on September 20, 2017, Air Force General John E. Hyten was asked about the threat of EMP attack on the United States. He told conference attendees US Strategic Command would be able to respond because its systems and facilities are hardened against EMPs, but every cell phone, computer, automobile, or anything else with a computer chip in it would be rendered useless. He went on to say, “[W]e have not looked at the critical infrastructure that could be damaged by EMP, and we need to kind of take a step back and look at that entire threat because it is a realistic threat.”⁷¹

An adversary could produce an EMP using two different methods. The first and most catastrophic method is by detonating a nuclear device in the atmosphere. The severity of the EMP’s effect is determined by the height of the blast. The higher the blast, the larger the affected area.⁷² According to estimates, a nuclear airburst EMP could cause trillions

66. National Defense Authorization, Fiscal Year 2001, Pub. L. No. 106-398 (2000).

67. Anu Narayanan et al., *Deterring Attacks against the Power Grid: Two Approaches for the US Department of Defense* (Santa Monica, CA: RAND Corporation, 2020), 13.

68. *Terrorism and the EMP Threat to Homeland Security: Hearing before the Subcommittee on Terrorism, Technology and Homeland Security of the Committee on the Judiciary*, 109th Cong. (2005) (statement of Lowell Wood, commissioner, Congressional Electromagnetic Pulse Commission).

69. *Terrorism and the EMP Threat*.

70. John Kester, “The Trump Administration Has No Plan for Dealing with a North Korean EMP Attack,” *Foreign Policy* (website), October 16, 2017, <https://foreignpolicy.com/2017/10/16/the-trump-administration-has-no-plan-for-dealing-with-a-north-korean-emp-attack/>.

71. “Hyten Speaks at AFA Conference,” speech, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, September 20, 2017, video, 59:43, September 21, 2017, <https://www.youtube.com/watch?v=3m691gCJWME>.

72. James Carlini, “Defending Critical Infrastructure against EMPs,” *Electrical Contractor* (website), July 2016, <https://www.ecmag.com/section/systems/defending-critical-infrastructure-against-emps>.

of dollars in damages to the power grid.⁷³ The detonation could also kill 90 percent of the US population.⁷⁴ Should the United States be attacked in this way, any forces left in the CONUS would be required to assist in recovery and would not be in a position to deploy.

The second way an adversary could use an EMP to attack the United States is with an “e-bomb” or nonnuclear electromagnetic pulse (NNEMP) device. These weapons use bursts of energy to disrupt or destroy electronic devices. An example of this device is the Counter-electronics High-powered Microwave Advanced Missile Project Boeing developed for the Air Force. These devices use a microwave pulse to destroy electronics.⁷⁵ An adversary intent on disrupting a strategic port during mobilization would not necessarily need to match the US Air Force in sophistication. Group Captain Atul Pant of the Indian Air Force claims a small-scale NNEMP device could easily be made using commonly available materials.⁷⁶ In a 2017 blog post, he stated, “[T]he biggest issue with non-nuclear EMP weapons is that the complexity and threshold required to produce them is minimal.”⁷⁷

A 2008 Heritage Foundation report paints a picture of the threat EMPs pose to the United States. The authors assert Russia has developed an EMP-emitting device that fits on a dining room table, and China has discussed the possibility of using EMP weapons in future conflicts.⁷⁸ Apparently, an EMP attack on US ports would be a distinct possibility in a major conflict with either of these two countries.

The United States’ vulnerability to EMP attack, whether localized or as part of a much larger attack, is based on the nature of the US power grid. A 2021 Department of Energy report stated, “The US electric power grid is one of the Nation’s critical life-line infrastructure on which many other critical infrastructure depend, and the destruction of this infrastructure can cause a significant impact to national security and the US economy.”⁷⁹ The United States needs to invest more in its power grid. Many US industrial control systems run on software that is a generation behind and not designed with cybersecurity in mind.⁸⁰ A cyberattack or EMP attack on one part of the power grid

73. Carlini, “Defending Critical Infrastructure.”

74. US Senate Committee on Homeland Security and Governmental Affairs, *Activities of the Committee on Homeland Security and Governmental Affairs* (Washington, DC: Government Publishing Office, 2017), 6.

75. George I. Seffers, “CHAMP Prepares for Future Flights,” SIGNAL, February 1, 2016, <https://www.afcea.org/content/Article-champ-prepares-future-fights>.

76. Atul Pant, “EMP Weapons and the New Equation of War,” *IDSA Comment* (blog), October 13, 2017, https://idsa.in/idsacomments/emp-weapons-new-equation-of-war_apant_131017.

77. Pant, “EMP Weapons.”

78. Jena Baker McNeill and Richard Weitz, *Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe* (Washington, DC: Heritage Foundation, October 20, 2008), 7.

79. Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the US Power Grid* (Washington, DC: Department of Energy, June 2012), vi.

80. Robert K. Knake, *A Cyberattack on the US Power Grid*, Contingency Planning Memorandum no. 31 (New York: Council on Foreign Relations, April 2017).

could have a cascading effect, turning a localized blackout into a widespread outage affecting millions.⁸¹

Given US adversaries have the ability to reach the continental United States with an EMP weapon or cyberattack on US infrastructure, the US government continues to work with private owner-operators of strategic ports and the rest of the nation's critical infrastructure. The Maritime Administration and Military Surface Deployment and Distribution Command designate certain seaports as strategic seaports because of their proximity to infrastructure such as roads, rail lines, and utilities; thus, a port's ability to support military shipments can be greatly reduced if the power for a rail line or road network is cut.

Given the challenges strategic ports face today, this chapter proposes steps that should be taken to increase the likelihood of the successful use of strategic ports for mobilization in a contested environment. The structural integrity of strategic seaports, physical security, cybersecurity (including GPS), and protection from EMPs are addressed.

Port operators or state and local authorities are usually responsible for the structural integrity of US ports. In the past, port owners and operators have had the opportunity to apply for Transportation Investment Generating Economic Recovery grants from the Department of Transportation. These grants, ranging from \$5 million to \$25 million, were used for the improvement or repair of port facilities.⁸² In 2021, the Department of Transportation transitioned to the Rebuilding American Infrastructure with Sustainability and Equity grant program, the maximum dollar amount of which is \$25 million. The grant is available to regional and local governments for transportation projects, providing a funding vehicle for needed infrastructure improvements.⁸³

Physical security has seen greater advancements than any other type of port security since the 9/11 attacks. The Security and Accountability for Every Port Act of 2006 was enacted to address port security concerns. Focusing primarily on the threat of terrorist attacks, the legislation has been most effective in addressing the physical security of ports.⁸⁴ Moreover, the US Coast Guard does a good job of overseeing the physical security of ports, as described in the 2014 testimony of Department of Homeland Security and US Coast Guard officials before the Senate Committee on Homeland Security and Governmental Affairs.⁸⁵ Congress continues to do its part by funding the Port Security Grant Program, which "provides funds for transportation infrastructure

81. Woodward, "Weak Links in US Power Grid."

82. Haylle Sok, "\$500 Million in New Funding Available through TIGER Program," *Global Trade* (website), September 8, 2017, <https://www.globaltrademag.com/500-million-new-funding-available-tiger-program/>.

83. "RAISE Discretionary Grants," US Department of Transportation (website), updated April 13, 2021, <https://www.transportation.gov/RAISEgrants>.

84. Willis, "Ten Years After."

85. *Evaluating Port Security*.

security activities to implement Area Maritime Security Plans and facility security plans” and covers cybersecurity and other physical security measures at ports.⁸⁶

Grants alone are not enough to protect US strategic ports from cyberattacks. One might assume the Coast Guard is not staffed or funded to handle the job of adding cyber to its physical security assessments of seaports. The Coast Guard works under the Department of Homeland Security during peacetime. As evidenced in the GAO reports previously cited, the Coast Guard is not performing its assessments of strategic seaports quickly enough. The Department of Homeland Security should provide the Coast Guard with additional resources to assist in completing the currently outstanding assessments. Perhaps the Cybersecurity & Infrastructure Security Agency National Cybersecurity Protection System could be tasked with assisting or augmenting US Coast Guard cyber personnel in the completion of the task. Companies need to know their systems are secure, and the Department of Defense needs to know its shipping data is not falling into the wrong hands. Further, Congress needs to know the extent of vulnerabilities to provide funding to correct them.

The Department of Defense could also help with the assessments. The mission of the National Guard Cyber Protection Teams is to coordinate, train, advise, and assist; thus, they could assist the Coast Guard in addressing seaport cybersecurity.⁸⁷ As a long-term solution, Military Surface Deployment and Distribution Command’s five transportation brigades could each be allocated one cyber protection team from US Army Cyber Command.⁸⁸ Each brigade would then have the ability to assist the commercial companies working with US Transportation Command. Developing the working relationships between port and shipping company cybersecurity personnel and the Military Surface Deployment and Distribution Command transportation brigades they collaborate with would be valuable. This route may be difficult since it would require the Department of the Army to make a force management decision. This option, however, should be explored.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, mandated the creation of the DHS Critical Infrastructure Cyber Community Voluntary Program and a risk-based Cybersecurity Framework, a set of industry standards and best practices to help organizations manage cybersecurity risks.⁸⁹ The department and industry should select and implement a single cybersecurity standard. In addition, the Critical Infrastructure Cyber Community Voluntary Program should be mandatory and a prerequisite for ports hoping to participate in the

86. Department of Homeland Security (DHS), “Fiscal Year 2017 Port Security Grant Program,” Maritime Security Outlook, n.d., https://www.maritimesecurityoutlook.com/images/2017_PSGP/FY_2017_PSGP_Fact_Sheet_FINAL_508.pdf.

87. Justin Berndt, “Minnesota Granted Exclusive Cyber Protection Team,” Cyber Security Summit, February 5, 2016, <https://cybersecuritysummit.org/2016/02/05/minnesota-granted-exclusive-cyber-protection-team/>.

88. “SDDC Organization,” US Army Military Surface Deployment & Distribution Command (website), n.d., <https://www.sddc.army.mil/sddc/Pages/org.aspx>.

89. Executive Order No. 13,636, 3 C.F.R. 13636 (2013); and DHS, *C3 Voluntary Program Outreach and Messaging Kit* (Washington, DC: DHS, 2014).

Strategic Seaport Program. Furthermore, Military Surface Deployment and Distribution Command should use the standards of the framework to evaluate prospective Ports for National Defense when each port study is conducted by the their Transportation Engineering Agency.⁹⁰ Also, the Maritime Administration should reinforce to private port operators the urgency of protecting the networks at strategic seaports through the National Port Readiness Network.

An EMP created by a nuclear detonation over the United States would be catastrophic and make deployment nearly impossible in the immediate aftermath, although this type of attack is not as likely to occur. As previously discussed, a more localized NNEMP attack could be used to impede mobilization to a strategic port. To mitigate this risk, an evaluation must be added to the Transportation Engineering Agency port survey that addresses the vulnerability of ports to a localized EMP device. Ports should then develop plans for hardening or shielding their systems from the effects of such an attack and develop a recovery plan in the event they are attacked before completing this hardening plan. These criteria should be required if the port is to be considered as a potential Port for National Defense.

Large power transformers are the single most critical link in the power grids that supply US ports. A recent Department of Energy study identifies the need for spare large power transformers and notes the relatively small number of manufacturers in the United States that can make these devices. Further, the study mentions the United States is too dependent on foreign suppliers for the devices.⁹¹ The Department of Energy must continue to work with the industry to ensure spare large power transformers are available in the event of an emergency.

A 2008 Heritage Foundation report examined the threat posed by EMPs to the US power grid. The report also discusses NNEMPs and their largely localized effects. Further, the foundation believes, “If properly shielded, electrical devices and systems can generally survive even the strongest EMPs.”⁹² Congress should ensure current grant programs for port security allow for EMP-shielding costs.

Conclusion

This chapter discussed threats that could seriously impede the Department of Defense’s mobilization and deployment of the US military through its designated strategic seaports. The evaluation criteria, the structural integrity of ports, and security at port facilities require additional consideration by the US government.

The evaluation criteria used by Military Surface Deployment and Distribution Command to select strategic seaports are based on scenarios that are no longer relevant. Military leadership can no longer assume the armed forces can mobilize from the continental United States uncontested. The new strategic environment, as described by former Secretary of Defense Mattis, is one in which the United States may enter into conflict with near-peer powers, and the efforts

90. SDDC, *Strategic Seaports Implementation Plan*, 2.

91. Office of Electricity Delivery and Energy Reliability, *Large Power Transformers*, v-vi, 6.

92. McNeill and Weitz, *Electromagnetic Pulse (EMP) Attack*.

of the Department of Defense to mobilize will be contested.⁹³ Thus, the evaluation criteria for the selection of strategic seaports need to change to reflect the new threat.

The structural integrity of US ports must be sufficient to support mobilization in all areas of the country. Previous assessments assumed outdated criteria and deployment rates that did not account for the current strategic environment as outlined in the current *National Defense Strategy*. As evidenced by the degraded conditions of the Port of Alaska, more work is needed to fix US ports. Both the military and commercial shipping companies would benefit from these improvements.

The security at US ports is perhaps the gravest shortfall. This topic is divided into two parts, and cybersecurity is the first part. Despite progress in physical security (fencing, security cameras, and guards), the Coast Guard has been unable to assess the civilian cybersecurity posture of the strategic seaports.⁹⁴ The threat to civilian systems is also a threat to the Department of Defense because civilian companies ship a large amount of DoD cargo. Information on these shipments is vulnerable because port networks are underprotected. In addition to computer systems, cameras, barcode readers, and other peripheral devices linked to port networks are vulnerable to intrusion, and GPS used by automation systems in ports, such as crane automation systems, are vulnerable to jamming. A whole-of-government approach must be taken to address the cyber issues—one that includes the Department of Defense, the Department of Homeland Security, and Congress.

The second part of port security is vulnerability to EMPs. Both nuclear weapons and NNEMPs pose a threat to the systems required to move military formations through the ports and onto ships. The technology to shield key devices exists and must be explored to protect against disruption during mobilization.

The recommendations proposed to address the structural and security issues are rudimentary and achievable. The criteria used to evaluate potential strategic seaports needs to be reevaluated against the new strategic environment. Cybersecurity and EMP resilience measures must be added to the criteria used by Military Surface Deployment and Distribution Command to select ports for DoD use. Congress must continue to fund grant programs meant to improve and secure the critical infrastructure at US ports.

93. Mattis, *Summary of 2018 National Defense Strategy*, 2–3.

94. Wilshusen and Caldwell, *Maritime Critical Infrastructure Protection*, 2–4.

4. SINGLE POINT OF FAILURE

Viewing national defense from the perspective of business has contributed to a culture within the Department of Defense (DoD) that values efficient processes above effectiveness and system redundancy.¹ The business systems approach is financially reasonable, but it may not make sense militarily. This approach, when applied to military operations, can create points that are vulnerable to exploitation by enemies of the United States; the approach also degrades the flexibility that may be needed when handling a crisis. The cumulative effect of logistics capability reductions across the services in the name of efficiency is far more significant when examined broadly than when viewed in isolation. The rise of near-peer adversaries is a great concern in the *National Security Strategy*.² The risk imposed by near-peer adversaries may diminish the value of efficiency and illuminate risks to US national security. A single point of failure may be identified and exploited by our adversaries in a time of crisis, thereby reducing our capacity to respond.

Culturally, Americans have become ingrained with a belief the US homeland is secure from enemy attack. The United States has friendly neighbors to the north and south and oceans to the east and west. For most of US history, the country has been relatively safe from enemy attacks or invasions into the homeland. The September 11 attacks and other terrorist attacks, however, have begun to alter this sense of security. The United States' ability to strike its enemies abroad and successfully deter attacks on its homeland has reinforced the sense of safety in Americans, creating opportunities for our adversaries. Any competent, capable foe would want to target an adversary's munitions infrastructure and supplies.

The rise of near-peer adversaries, such as Russia and China, with the resources to locate and exploit vulnerabilities in the munitions logistics process, requires the United States to reassess its cost-versus-risk criteria for crucial infrastructure. A business mindset that focuses on efficiency and removal of redundant capabilities may narrow the targets of enemies.³ Determining an exploitable point of failure within the logistics nodes handling munitions for the US military will likely be accomplished by capable adversaries. Munitions are the most vulnerable class of supply to attack and, naturally, have more restrictions than other commodities.⁴ The United States must reexamine how it can prevent attacks, protect its logistics infrastructure, mitigate the effects of attacks, and recover from attacks.⁵

1. Everett C. Dolman, "On the Business Models of War," *Strategy Bridge*, November 22, 2017, <https://thestrategybridge.org/the-bridge/?author=56fdec1037013b09a736eeda>.

2. Donald Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), 46–48.

3. Dolman, "Business Models of War."

4. Headquarters, Department of the Army (HQDA), *Materiel Management, Supply, and Field Services Operations*, Army Techniques Publication (ATP) 4-42 (Washington, DC: HQDA, November 2020), 1-3.

5. Department of Homeland Security (DHS), *National Response Framework*, 3rd ed. (Washington, DC: DHS, June 2016), 1.

PREVENTION

Preventing an attack on the munitions supply and distribution chain requires constant vigilance and information sharing among the federal, state, and local levels of government. To prevent an attack, the United States must determine credible threats to the force projection of munitions and how enemies will potentially exploit vulnerabilities. Preventing an attack on US munitions ports and supporting infrastructure requires acknowledging the growing threat to the homeland and actively including this mindset into plans and preventative measures, such as the layered approach currently used by the Department of Homeland Security (DHS).⁶ The layered approach “has entailed the creation of a framework that uses a layered strategy to vet transportation workers, vessels, cargo, and crew, beginning at the international origin and continuing throughout the global supply chain.”⁷ The Department of Defense should reexamine the risk to mission effectiveness and the cost of becoming a harder target with redundant capabilities. Finally, reviewing vulnerabilities externally and internally will possibly reveal insider threats and cybersecurity are the greatest concerns. According to Everett C. Dolman, “Part of the challenge that America faces is a business approach that stresses efficiency.”⁸ According to the think tank the Lexington Institute, “[W]hile reducing excess capacity measured in terms of current requirements is desirable, it is more important to maintain a capability to respond rapidly to unplanned and changing circumstances. In peacetime, the focus is naturally on efficiency and minimizing costs. In wartime, the measures of success must be effectiveness and timeliness.”⁹

To counter the efficiency mindset and prevent attacks on the homeland’s munitions assets, the Department of Defense may have to show Congress the credible threats the US critical munitions nodes are facing. In a resource-constrained environment, the case for investment in prevention must be made to justify expenditures in security enhancements.¹⁰ In this case, the justification is the capabilities of China, North Korea, and Russia.¹¹ These countries have demonstrated their capabilities, especially in cyberwarfare, and have been identified by the Defense Science Board as credible threats and thus can be held up as examples.¹²

6. Evaluating Port Security: Progress Made and Challenges Ahead, 113th Cong. (2014) (statement of Stephen L. Caldwell, Director, Homeland Security and Justice, Government Accountability Office).

7. Evaluating Port Security.

8. Dolman, “Business Models of War.”

9. Lexington Institute, *Supplying Ammunition: The Lifeblood of the Military* (Arlington, VA: Lexington Institute, November 2004), 5.

10. Larry Wyche and Greg Pieratt, *Securing the Army’s Weapon Systems and Supply Chain against Cyber Attack*, ILW Spotlight 17-3 (Washington, DC: Institute of Land Warfare, November 2017), 2.

11. Defense Science Board, *Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017), 26–28.

12. Defense Science Board, *Task Force on Cyber Deterrence*.

To make the United States a harder target and less vulnerable to attack, the prioritization of efficiency needs to give way to maintaining redundant, less efficient capabilities.¹³ Redundancy in capabilities will frustrate an adversary's ability to disrupt military operations. Excess and dispersed capabilities have a preventative impact on their own. If an asset is redundant, would it meet the payoff-versus-risk calculus of our adversaries? Redundancy reduces the targeting threat. Opponents naturally look for the most limiting areas to attack. Concentrating capabilities in a few geographic locations creates targets, such as the two munitions ports located on the East and West Coasts of the continental United States.

A potential, concerning Russian action for the munitions discussion is the destruction of a munitions depot in Ukraine in 2017. The massive explosion possibly resulted from an insider act of sabotage.¹⁴ A nonconventional or gray-zone attack that could be denied by our enemies is a possibility on American soil.¹⁵ Gray-zone attacks "are frequently shrouded in misinformation and deception, and are often conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down."¹⁶ A well-executed, unconventional assault is difficult to prove and easy to execute, especially with the backing and resources of nations such as China and Russia.

The US military must always consider insider threats when examining US port security systems.¹⁷ The actions of Edward Snowden and the damage he inflicted to national security should make the United States reflect on the real possibility of insider threats and the risk they present to the security of vital US munitions ports.¹⁸ The volume of containers arriving at US munitions ports from road, rail, air, and sea precludes personnel from physically inspecting all containerized cargo.¹⁹ A layered system identifies high-risk containers based on the country of origin, and inspection resources focus on the countries highlighted in intelligence reports.²⁰ The lack of inspection

13. Lexington Institute, *Supplying Ammunition*, 5.

14. Roland Oliphant and Charlotte Krol, "Huge Explosion at Ukraine Ammunition Depot Prompts Mass Evacuation," *Daily Telegraph*, September 27, 2017, <http://www.telegraph.co.uk/news/2017/09/27/fire-ukraine-ammunition-depot-prompts-mass-evacuation/>.

15. Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute (website), February 5, 2016, <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/#>.

16. Brands, "Paradoxes."

17. Jayson Ahern, "Port Security in the Cyber Age," Cipher Brief (website), April 6, 2016, <https://www.thecipherbrief.com/port-security-in-the-cyber-age>.

18. Ahern, "Port Security."

19. US Customs and Border Protection (CBP), "Cargo Examination," CBP (website), updated May 15, 2017, <https://www.cbp.gov/border-security/ports-entry/cargo-security/examination>.

20. CBP, "Cargo Examination."

capacity creates a vulnerability.²¹ An insider could readily provide information on the types of uninspected containers and enable an attack on a key port.²²

External threats are also present, especially when examining the cyber domain, and valuable information can be gathered to find a weak link. North Korea has launched successful cyberattacks without possessing the resources China and Russia have.²³ Security is considered to be crucial, but excess capacity is seen as wasteful when viewed through the business mindset that permeates current military thinking.²⁴ Cybersecurity is growing in importance and its maintenance is essential to prevent attacks. Hackers and the ever-increasing automation of global shipping have made the maritime domain increasingly vulnerable.²⁵ Streamlining costs via automation has resulted in massive container vessels operated with minimal crews, which creates a perfect environment for a cyberattack.²⁶ As Jayson Ahern stated in an article on the Cipher Brief website:

The US Coast Guard has taken actions to improve cybersecurity at ports, including the August 2015 roll out of a Cyber Strategy aimed at defending ports, companies, and infrastructure from cyberattacks. The uncovering of a 2013 drug smuggling operation in which smugglers successfully hacked cargo tracking systems at the Port of Antwerp to avoid detection, as well as a seven-hour [Global Positioning System (GPS)] signal disruption that shut down operations of a major US port in 2014, demonstrate the seriousness of the cyber threat.²⁷

Preventing an attack by active cyber detection and risk management is part of the solution, but the United States must also put protective measures in place.

PROTECTION

Protecting the US munitions infrastructure is a fundamental part of successfully preserving the country's capacity to fight. The defense against such attacks is primarily outside the realm of the Department of Defense and is the responsibility of either the Department of Homeland Security and federal agencies or local law enforcement.²⁸ According to Homeland Security Presidential Directive 7, "In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary [of DHS] shall

21. Wendy J. Keefer, "Container Port Security: A Layered Defense Strategy to Protect the Homeland and the International Supply Chain," *Campbell Law Review* 30, no. 1 (October 2007): 140-42.

22. Ahern, "Port Security."

23. Defense Science Board, *Task Force on Cyber Deterrence*, 27-28.

24. Dolman, "Business Models of War."

25. Jeremy Wagstaff, "All at Sea: Global Shipping Exposed to Hacking Threat," Reuters (website), April 23, 2014, <https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424>.

26. Pietro Savo, "Homeland Security by Sea, by Air, by Land," LinkedIn, April 20, 2016, <https://www.linkedin.com/pulse/homeland-security-sea-air-land-dr-pietro-pete-savo>.

27. Ahern, "Port Security."

28. Eric V. Larson and John E. Peters, *Preparing the US Army for Homeland Security* (Santa Monica, CA: RAND Corporation, 2001), 158.

be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States.”²⁹

Overall protection is a shared responsibility among the Department of Defense, Department of Homeland Security, and state and local authorities.³⁰ The National Guard can also play an essential role by providing additional security assets, including aircraft for surveillance, explosive ordnance disposal teams, and other capabilities that can augment civilian law enforcement agencies in a time of crisis.³¹ Protecting munitions can also be achieved by producing arms in a manner that decreases vulnerability to attack.³² A near-peer adversary will have likely identified US force projection capabilities, including “logistics nodes such as ports, airheads, and ammunition storage areas as key targets for enemy attack” and a center of gravity to disable in a confrontation with the United States.³³ According to Robert A. Rossi of the US Army Defense Ammunition Logistics Activity, “The Army Armament Research Development and Engineering Center (ARDEC) concluded that the munitions logistics system is severely vulnerable to disruption during initial buildup in wartime operations due to enemy attack.”³⁴ Adversaries could potentially focus their efforts on munitions, and an asymmetric attack, including a terrorist attack, is a possible course of action.³⁵

The US Coast Guard is responsible for protecting US ports.³⁶ The growing cyber threat is very concerning because of the high degree of automation in the shipping industry. Currently, “the United States Coast Guard—does not have specific authority to regulate cybersecurity in port facilities or any other area of maritime critical infrastructure.”³⁷ The lack of cybersecurity authority within the US Coast Guard creates a gap that can be exploited in the future if the issue is not addressed. The Coast Guard and other law enforcement agencies have a role in protecting DoD munitions assets. The Department of Defense must interact with the Department of Homeland Security and local law enforcement to ensure the protection of munitions infrastructure and movements. In the homeland, the Department of Defense depends on law enforcement and coordinates with other agencies to ensure protection.³⁸ Fortunately, fusion centers exist to facilitate broad coordination across the Department of Defense and the federal, state,

29. George W. Bush, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (Washington, DC: White House, December 17, 2003).

30. Bush, *Critical Infrastructure Identification*.

31. Larson and Peters, *Preparing the US Army*, 147.

32. Robert A. Rossi, *The Army Munitions Survivability Program* (Picatinny Arsenal, NJ: US Army Defense Ammunition Logistics Activity, August 1996), 1.

33. Rossi, *Army Munitions Survivability Program*.

34. Rossi, *Army Munitions Survivability Program*, 1–2.

35. Rossi, *Army Munitions Survivability Program*.

36. Ahern, “Port Security.”

37. Joseph Kramek, *The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities* (Washington, DC: Brookings Institution Press, July 2013).

38. Larson and Peters, *Preparing the US Army*, 158.

and local levels of government. According to a DHS press release, “State and major urban area fusion centers provide critical links for information sharing between and across all levels of government.”³⁹

Despite the provision of financial support by the federal government, a lack of resources and the immense area that must be protected at the state and local levels create gaps and seams adversaries could exploit. To address possible gaps in infrastructure security, the FBI has improved information sharing with local law enforcement.⁴⁰ The US military has more resources than any other agency for addressing a weak link, but posse comitatus is a limiting factor that restricts DoD law enforcement functions.⁴¹ The FBI may request a waiver to posse comitatus when the Bureau requires law enforcement support from the US Army, US Navy, and US Air Force.⁴² The National Guard, when acting under Title 32 of US Code, and the Coast Guard, in peacetime, are not subject to the Posse Comitatus Act and can be used to protect potential gaps, especially in surveillance and detection activities.⁴³ More planning and war gaming are needed to identify likely soft spots that require more protection.

Significant effort has been initiated since the September 11 attacks to ensure US infrastructure and munitions ports are safe and secure.⁴⁴ An attack on Military Ocean Terminal Sunny Point on the East Coast or Military Ocean Terminal Concord on the West Coast would be difficult, but not be impossible.⁴⁵ An asymmetric attack from a near-peer adversary with vast resources at its disposal is a possibility we must be prepared to address. An attack on critical logistics nodes would be possible in an armed conflict with state or nonstate aggressors.⁴⁶

Protecting munitions infrastructure also includes producing munitions that are safer to handle, ship, and store. The Army initiated the Munitions Survivability Program

39. Office of the Press Secretary, “DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism,” DHS, September 14, 2009, <https://www.dhs.gov/news/2009/09/14/new-information-sharing-tool-fusion-centers-announced>.

40. Office of the Inspector General Audit Division, *The Federal Bureau of Investigation’s Efforts to Improve the Sharing of Intelligence and Other Information*, Audit Report 04-10 (Washington, DC: Department of Justice, December 2003), iv.

41. Larson and Peters, *Preparing the US Army*, 243–44.

42. “1614. Posse Comitatus Waiver—18 U.S.C. 351” US Department of Justice Archives, updated January 17, 2020, <https://www.justice.gov/usam/criminal-resource-manual-1614-posse-comitatus-waiver-18-usc-351>.

43. Larson and Peters, *Preparing the US Army*, 244.

44. Office of the Inspector General Audit Division, *The Federal Bureau of Investigation’s Efforts to Protect the Nation’s Seaports*, Audit Report 06-26 (Washington, DC: Department of Justice, March 2006), i–iii.

45. Kimberly Hanson, “Military Ocean Terminals Play Strategic Role in Defense,” US Army (website), October 17, 2013, https://www.army.mil/article/113348/military_ocean_terminals_play_strategic_role_in_defense.

46. Office of the Inspector General Audit Division, *Federal Bureau of Investigation’s Efforts*, ix.

to address safety issues in munitions manufacturing.⁴⁷ The program identifies ports, airheads, and ammunition storage areas as critical targets for enemy attack.⁴⁸ The United States now produces munitions in a manner that reduces the possibility of explosions and susceptibility to detonation by outside sources.⁴⁹ Rossi's report on the program, however, focuses on threats from adversaries in forward storage locations and fails to recognize risks would also be met domestically in the homeland.

A port, by its very nature, faces threats from land, sea, and air.⁵⁰ Adversaries may not have to disable the port itself; choke points, such as canals, are less secure, but they are essential for the port to function successfully. Incoming cargo is a threat to US munitions terminals since cargo comes in a variety of forms, causing a great deal of turbulence and frustration.⁵¹ A near-peer or capable adversary may not allow the United States to project forward and build combat power, and will seek to challenge the United States on its soil. According to Barry D. Watts at the Center for Strategic and Budgetary Assessments, "China's growing cyber capabilities are not only enabling the theft of US intellectual property and military secrets but could provide the [People's Liberation Army] with the means to impose severe damage on the US infrastructure."⁵² Collectively, the US military needs to reexamine its munitions infrastructure through the eyes of a peer adversary to determine the amount of risk the infrastructure faces. According to Larry Wyche and Greg Pieratt, "The Army should apply the same level of effort that it invests in safeguarding its networks and information systems toward protecting its armaments and its ability to sustain them."⁵³

MITIGATION

A US vulnerabilities mitigation strategy cannot merely focus on one aspect of munitions logistics. Port capabilities and capacities, available lift, skilled labor, alternate locations, storage locations, and the industrial base are areas that require consideration.⁵⁴ Redundancy is severely lacking in the US logistics system architecture as well as the capacity for surge capacity.⁵⁵ During the Persian Gulf War,

47. Rossi, *Army Munitions Survivability Program*, 1.

48. Rossi, *Army Munitions Survivability Program*, 1.

49. Rossi, *Army Munitions Survivability Program*, 1.

50. Keith Laing, "Lawmakers Fret about Potential Terrorist Attacks at US Ports," *Hill* (website), October 27, 2015, <http://thehill.com/policy/transportation/258290-lawmakers-fret-about-potential-terrorist-attacks-at-us-ports>.

51. Keefer, "Container Port Security," 140–42.

52. Barry D. Watts, *Sustaining the US Defense Industrial Base as a Strategic Asset* (Washington, DC: Center for Strategic and Budgetary Assessments, September 2013), 5–6.

53. Wyche and Pieratt, *Securing the Army's Weapon Systems*, 2.

54. Sarah Garner, "Record of Decision for the Modernization and Repair of Piers 2 and 3, Military Ocean Terminal Concord, CA," *Federal Register* 80, no. 89 (May 8, 2015): 4.

55. Craig Dunlap, "Port Munitions Backlog Brings ILA Volunteers," *Journal of Commerce* (website), February 7, 1991, www.joc.com/port-munitions-backlog-brings-ila-volunteers_19910207.html.

Military Ocean Terminal Sunny Point served as the primary port for shipping munitions, but it could not keep pace with the demand, causing delays.⁵⁶ To address the problem, the Army paid for high-speed cranes that have increased the processing capacity of the port and reduced manpower requirements.⁵⁷ As another benefit, the cranes decreased risk by processing munitions quickly and preventing backlogs.⁵⁸

Removing a munitions port from either coast may require munitions to transit the Panama Canal, which Chinese-owned companies essentially control. According to Yojiro Konno and Nancy Menges, "It is highly plausible that [the Chinese-owned company] Hutchison Whampoa has the potential to act as Beijing's political agent and that their possession of the ports at either end of the Panama Canal constitutes a serious US national security issue."⁵⁹ Also, according to Christopher J. McMahon, "China controls more ports and terminals around the world than any other nation, including terminals on both sides of the Panama Canal."⁶⁰

Alternative ports in the United States are available for munitions, but these ports present much higher risk to port operations. For example, as a result of Military Ocean Terminal Concord being in disrepair, the Army considered an alternate port on the West Coast; the Army also considered Military Ocean Terminal Sunny Point as a backup. Ultimately, these proposals were rejected for logistics and safety reasons, among others.⁶¹ Military Ocean Terminal Concord is the only West Coast port capable of safely handling munitions.⁶² Neutralizing these terminals in some fashion would possibly reduce the United States' ability to respond quickly to an attack. A focus on efficiency has possibly created a vulnerability our enemies can exploit.

The Army should assess the viability of alternate ports and identify potential negative issues before using the ports. The military needs to conduct logistics training operations to test capabilities. Actual use is the best way to identify and address deficiencies at alternate locations. Many shortcomings become apparent only when putting a plan into practice. Driven by efficiency, the military has focused on high-speed equipment at two locations on opposite coasts that can process munitions quickly.

If these ports are eliminated, what is the speed and capability of cranes at alternate locations? Can they do the same job or will munitions handlers be required? Many of these answers are not broadly known, but they could be explored by using alternative ports. Coordinating for alternate locations can involve expansion of the workforce and increased security the military must coordinate through the Military

56. Dunlap, "Port Munitions Backlog."

57. Hanson, "Military Ocean Terminals."

58. Hanson, "Military Ocean Terminals."

59. Yojiro Konno and Nancy Menges, "China's Control of the Panama Canal Revisited," *Menges' Americas Report* (blog), October 6, 2008, <http://themengesproject.blogspot.com/2008/10/chinas-control-of-panama-canal.html>.

60. Christopher J. McMahon, "The US Merchant Marine: Back to the Future?," *Naval War College Review* 69, no. 1 (Winter 2016): 102.

61. Sarah Garner, "Record of Decision," 4.

62. Hanson, "Military Ocean Terminals."

Surface Deployment and Distribution Command.⁶³ Fortunately, the command has the Strategic Seaport Program to address the need for surge capacity.⁶⁴ According to the command, “The [Strategic Seaport Program] is a key component to transportation and materiel readiness. It enables surge deployments and responses to national security contingencies by providing a reserve seaport capacity to meet elevated demand for military cargo.”⁶⁵ Though the command has port assessments for alternate locations, using an alternate location as part of a force rotation involving munitions could potentially confirm those assessments.

A robust sealift and workforce capability to process munitions and project forward may be critically important and could enable the use of multiple smaller ports to either augment or replace a munitions seaport if it is disabled by adversaries. Unfortunately, the United States’ once-robust sealift availability and capacity have declined since the Cold War.⁶⁶ The US Merchant Marine and vessels under contract have significantly degraded. In 2015 Chris Dupin wrote, “There were more than 1,200 such ships just after World War II. The fleet had fallen to about 200 in the 1980s, to 100 a year ago and to about 80 today.”⁶⁷ In a contested environment, this lack of capability would be a vulnerability exploited by a near-peer adversary.⁶⁸ A conflict with a near-peer adversary would naturally spill over into economics and trade relations, forcing countries with sealift capabilities to choose sides.⁶⁹

The US Merchant Marine is underfunded by the federal government. Currently, “the US Merchant Marine receives only a minuscule amount of federal support. It is certainly not enough to encourage the expansion of the US-flag fleet.”⁷⁰ The US Merchant Marine needs revitalization to counter the global shipping business shift, which currently favors the Chinese.⁷¹ Can the United States merely contract for additional sealift? This assumption may no longer be viable. Many companies and countries may not want to support US military operations, primarily if the United States were in a confrontation with a near-peer adversary, such as China.⁷² If companies or nations assist the United States, they could lose the support and business of an adversary. Supporting the United States in a conflict may not be worth the cost for many countries or organizations

63. SDDC, “Strategic Seaport Program,” STAND-TO!, US Army (website), February 28, 2017, https://www.army.mil/standto/archive_2017-02-28.

64. SDDC, “Strategic Seaport Program.”

65. SDDC, “Strategic Seaport Program.”

66. McMahon, “US Merchant Marine,” 95–96.

67. Chris Dupin, “The US Merchant Marine in Serious Decline,” *American Shipper* (website), April 16, 2015, https://americanshipper.com/main/news/us_merchant_marine_in_serious_decline_60006.aspx.

68. McMahon, “US Merchant Marine,” 97.

69. McMahon, “US Merchant Marine,” 101.

70. McMahon, “US Merchant Marine,” 105.

71. McMahon, “US Merchant Marine,” 102.

72. McMahon, “US Merchant Marine,” 101.

that also trade with US adversaries.⁷³ This effect occurred previously with Russia's economy, which is much smaller than China's economy. Many European allies were hesitant about taking a firm stance against Russian aggression after the Ukraine crisis.⁷⁴ As China grows in power and prominence and more companies and countries' economies become more dependent on Chinese trade than on US trade, supporting US efforts may become too costly.⁷⁵

To mitigate the loss of a port, airlift is the fastest, most flexible, and most expensive means to ship munitions, but this method would not mitigate the loss of either Military Ocean Terminal Sunny Point or Military Ocean Terminal Concord.⁷⁶ Shipping munitions via aircraft is necessary for the highest-priority pieces, but aircraft cannot move enough stock to meet the requirements of a response to an attack by a potent adversary.⁷⁷ Airlift may also be in high competition for the prioritization of supplies and personnel, and the military does not have enough aircraft to supply the quantities of ammunition likely needed to respond to an attack on the homeland. Using airlift as a primary method of transporting munitions is not feasible.⁷⁸

In addition to revitalizing the US Merchant Marine, the military must monitor foreign ownership of rail and truck transportation assets and maintain discipline in this area. Fortunately, regulation has ensured US control of railroad dispatching.⁷⁹ According to the Code of Federal Regulations, "[I]n the absence of a waiver . . . all dispatching of railroad operations that occur in the United States [must] be performed in the United States, with two minor exceptions. First, a railroad is allowed to conduct extraterritorial dispatching from Mexico or Canada in emergency situations, but only for the duration of the emergency."⁸⁰ Rail can be used to ship munitions to alternate locations or across the country, if necessary. The US' freight rail system is in excellent condition.⁸¹

Labor capacity must be increased to mitigate effectively the results of an attack on the US munitions infrastructure.⁸² During the Persian Gulf War, the military could not

73. McMahon, "US Merchant Marine," 101.

74. Katie Simmons, Bruce Stokes, and Jacob Poushter, "NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid," Pew Research Center (website), June 10, 2015, <https://www.pewresearch.org/global/2015/06/10/nato-publics-blame-russia-for-ukrainian-crisis-but-reluctant-to-provide-military-aid/>.

75. McMahon, "US Merchant Marine," 101.

76. Robert T. Brigantic and Jean M. Mahan, *Defense Transportation: Algorithms, Models, and Applications for the 21st Century* (Amsterdam: Elsevier Science, 2004), 760-61.

77. Brigantic and Mahan, *Defense Transportation*.

78. Brigantic and Mahan, *Defense Transportation*.

79. US Locational Requirement for Dispatching of US Rail Operations, 49 C.F.R. 241 (2003).

80. US Locational Requirement.

81. Michael Grunwald, "Back on Tracks," *Time* (website), July 9, 2012, <https://business.time.com/2012/07/09/us-freight-railroads/>.

82. Dunlap, "Port Munitions Backlog."

move enough munitions through Military Ocean Terminal Sunny Point to keep pace with the demand, and the terminal has lost manpower since then.⁸³ Is contracting for munitions handlers a viable option if one of the primary ports is destroyed? A continual justification for the reduction of munitions-capable units and an option is contracting logistics capabilities, including material-handling equipment or sealift. During the Persian Gulf War, a shortage of skilled labor caused munitions stocks to back up, creating security and safety concerns.⁸⁴ In addition, these labor shortages occurred at a time when the military was much larger and more flexible than it is today.⁸⁵ A significant drawdown of forces has reduced the private pool available for companies' recruiting efforts. Furthermore, the demand for skilled munitions handlers in the active-duty Army has diminished because of outsourcing to contractors.⁸⁶ Contracting could cause delays because new personnel need to be trained. Also, more time would likely be required to award contracts and train personnel, even if these processes were rushed, and the US response time in an attack could be delayed as a result.

If necessary, to mitigate the effects of an attack, Joint Logistics Over-the-Shore could be used to establish an alternate location or to operate from a strategic port such as Military Ocean Terminal Sunny Point or Military Ocean Terminal Concord if it had been damaged in an attack.⁸⁷ A logistics rehearsal of concept (ROC) helps to identify munitions vulnerabilities or shortfalls. US Army Sustainment Command has hosted ROC drills in the past and gathered many lessons learned.⁸⁸ Joint and multinational ROC drills involving the United States' closest allies may also prove beneficial. If the US military shifted to an alternate port location, what would be the impact on other commodities? Perhaps this question and others can be answered by conducting further exercises, which provide valuable information to help determine the risk inherent in the United States' current munitions logistics posture. Conducting exercises and publishing the results at the unclassified level broadens the audience for lessons learned.

Another avenue to explore is the storage locations for munitions. Currently, the the military stores most munitions within the continental United States, keeping more money in the US economy and eliminating the requirement to maintain ammunition supply points on foreign soil.⁸⁹ Storing munitions in the continental United States may

83. Dunlap, "Port Munitions Backlog."

84. Dunlap, "Port Munitions Backlog."

85. Dunlap, "Port Munitions Backlog."

86. Thomas S. Schorr Jr. and Kenneth Deal, "Ammunition Management: A Joint or Army Function?," *Army Sustainment* 42, no. 4 (July–August 2010).

87. United States Transportation Command, "Joint Logistics Over-the-Shore: USTRANSCOM & JLOTS Program Update" (PowerPoint presentation, Transportation Research Board 26th Annual Summer Ports, Waterways, Freight & International Trade Conference, 2001), 3, <https://onlinepubs.trb.org/online-pubs/archive/conferences/2001SummerPorts/Session5Adams.pdf>.

88. Megan M. McIntyre, "ASC Hosts Ammunition ROC Drill," US Army (website), February 23, 2011, https://www.army.mil/article/52299/asc_hosts_ammunition_roc_drill.

89. HQDA, *Munitions Support in the Theater of Operations*, Army Field Manual 9-6 (Washington, DC: HQDA, March 20, 1998), 2-1.

make targeting of ports a stronger consideration for adversaries. Storing munitions out of the reach of adversaries is arguably safer, but the United States may be vulnerable in the homeland as well. The nation may not have the capabilities it once did to project munitions forward rapidly. A reduced projection capability increases the likelihood of munitions being destroyed by adversaries, even if they are stored farther away from the source of danger.

Conversely, storing munitions forward outside of the United States and closer to the threat reduces the number of munitions to be processed for deployment and the competition with other resources that are deploying. Prepositioned stocks and munitions are gaining increased attention, but they require a significant amount of resources.⁹⁰ In October 2016, the United States shipped over 600 containers of munitions to Germany to help set the European theater to deter Russian aggression.⁹¹ Munitions storage depots abroad have been allowed to decay and do not have the capacity and stockage levels they once did.⁹² Redundancy and disbursement merit further consideration when investigating munitions vulnerabilities and storage locations. Forward storage would ease the cumbersome process of moving massive amounts of munitions and other supplies forward in a timely matter.

The fall of the Soviet Union made the United States the undisputed world hegemon.⁹³ Congress and military leaders could likely not see the justification for maintaining an expensive global posture with multiple munitions-capable ports on both coasts.⁹⁴ Simultaneously, justifying the costs of storing massive amounts of munitions outside the United States was difficult, and the military and Congress began reducing military infrastructure.⁹⁵ Eventually, munitions-capable ports in the continental United States were streamlined, leaving only two available ports—one on the East Coast and one on the West Coast. Munitions storage shifted from a robust forward capacity abroad to a posture of storing most munitions within the continental United States. In Europe, only a single theater bulk munitions storage remains.⁹⁶

As the threat of a belligerent Russia reemerged, coupled with a nuclear-weapon-armed North Korea and a rising China, many planners realized the United States did not have enough munitions storage capacity abroad to sustain combat operations

90. HQDA, *Munitions Support*, 2-1.

91. Jacob McDonald, "The Biggest Ammo Shipment in 20 Years Arrives in Germany," US Army (website), November 8, 2016, https://www.army.mil/article/177936/the_biggest_ammo_shipment_in_20_years_arrives_in_germany.

92. Jen Judson, "Army Concerned over Shrinking Munitions Stockpile," *Defense News* (website), March 8, 2017, <https://www.defensenews.com/digital-show-dailies/global-force-symposium/2017/03/08/army-concerned-over-shrinking-munitions-stockpile/>.

93. Stacie L. Pettyjohn, *US Global Defense Posture, 1783–2011* (Santa Monica, CA: RAND Corporation, 2012), 83–89.

94. Pettyjohn, *US Global Defense Posture*.

95. Pettyjohn, *US Global Defense Posture*.

96. Pettyjohn, *US Global Defense Posture*, 90.

in an enduring conflict with a near-peer adversary.⁹⁷ Russia's annexation of Crimea and invasion of eastern Ukraine under the guise of independence fighters coordinating with ethnic Russian militias caught Europe off guard and sent a wake-up call throughout Europe and to the United States.⁹⁸ Vladimir Putin's invasion of Ukraine and pattern of belligerence has coincided with China's aggressive territorial claims in the South China Sea. Adversaries of the United States noticed the uncontested buildup of US forces in Iraq and the devastating results for the country in not challenging the United States. A strong adversary such as China or Russia would adapt and not repeat Saddam Hussein's mistakes.⁹⁹

Retaining US industrial capacity is critical for preventing and mitigating the effects of an attack on the US munitions infrastructure. Many leaders now realize the importance of the industrial base; this realization is apparent in the *National Security Strategy* released by the Trump administration.¹⁰⁰ Unfortunately, "the period from the end of the Cold War to present saw a 68 percent reduction in the overall capacity of the munitions industrial base."¹⁰¹

The United States cannot afford further decline and must reinvest in its munitions infrastructure.¹⁰² Complicating matters further is the severe impact the Iraq War, the Afghanistan War, and the Syrian Civil War have had on US munitions stores, reducing munitions stocks more quickly than factories are replenishing them. In 2010, the lack of industrial capacity and shortages began to impact combat operations. According to Thomas S. Schorr Jr. and Kenneth Deal, "The industrial base cannot manufacture preferred precision munitions on a grand scale, nor can it afford to. Many preferred munitions, such as Hellfire missiles and 30-millimeter high-explosive dual-purpose rounds, and common items, such as caliber .50 armor-piercing-incendiary rounds, are in short supply and have had, or are currently under, controlled supply rates."¹⁰³ According to a 2017 article on the Army's website, Lieutenant General Aundre F. Piggee stated "'preferred munitions'" were still in short supply, including munitions "used for the Patriot and Terminal High Altitude Area Defense systems, as well as Hellfire missiles and Excalibur rounds used for howitzers."¹⁰⁴

US European Command, US Pacific Command, and US Central Command have the strongest demand for munitions stocks, with all three commands needing

97. Judson, "Army Concerned."

98. Judson, "Army Concerned."

99. Robert Farley, "What Scares China's Military: The 1991 Gulf War," *National Interest* (website), November 24, 2014, <https://nationalinterest.org/feature/what-scares-chinas-military-the-1991-gulf-war-11724>.

100. Trump, *National Security Strategy*, 29–30.

101. Lexington Institute, *Supplying Ammunition*, 2.

102. Judson, "Army Concerned."

103. Schorr and Deal, "Ammunition Management."

104. David Vergun, "More Munitions, Prepositioned Stocks Big Priorities, Says G-4," US Army (website), March 17, 2017, https://www.army.mil/article/184023/more_munitions_prepositioned_stocks_big_priorities_says_g_4.

increases to existing stocks to counter threats effectively.¹⁰⁵ Shortages at these commands have revealed the US supplies need to be increased, and if a significant conflict arises, the US industrial base would need to expand. Consequently, newly produced stocks, along with existing supplies, may get processed through ports such as Military Ocean Terminal Sunny Point and Military Ocean Terminal Concord. In 2004, the Lexington Institute wrote:

No part of the defense industrial base is more critical to the success of the US military in conflict than that which produces munitions. At its most basic level, the function of the US military in conflict is to place energy on targets. Everything else that the military does is to create the conditions that will allow sufficient energy to be deposited in a timely manner on such targets, the destruction of which will lead to the defeat of any enemy. It is ammunition that makes the military an instrument of war.¹⁰⁶

Today, the US military stores and produces most of its munitions in the continental United States and must, therefore, have a robust logistics capability to project munitions forward in the event of a military crisis.¹⁰⁷ Efforts are underway to address this issue by increasing munitions stocks at forward bases.¹⁰⁸ Exercising contingency plans, however, may reveal the assumption that munitions-handler contractors will be readily available is flawed. In addition, having only two munitions ports, one on each coast, perhaps indicates the US military has assumed the homeland is uncontested. The Munitions Survivability Program was initiated to address perceived munitions risks during the Bosnian War and the Persian Gulf War.¹⁰⁹ Near-peer adversaries may not allow the United States to build combat power uncontested as Saddam Hussein did in the Persian Gulf War, and they could challenge and disrupt US operations in the continental United States in a variety of ways, including hybrid warfare and cyberattacks in combination with conventional methods.¹¹⁰ Perhaps the United States should consider the capabilities of near-peer adversaries to strike the homeland and adjust the Munitions Survivability Program accordingly.

RECOVERY

How can the United States increase its resiliency to an attack on its essential logistics infrastructure? The logistics capabilities of the US military and its ability to project power have been distinguishing characteristics of the United States over its adversaries. These capabilities have vulnerabilities, as stated above; thus, they should be protected and resourced by shifting more of the logistics assets that handle munitions to active status as opposed to reserve status or dramatically reducing reserve mobilization

105. Judson, "Army Concerned."

106. Lexington Institute, *Supplying Ammunition*, 1.

107. HQDA, *Munitions Support*, 2-1.

108. McDonald, "Biggest Ammo Shipment."

109. Rossi, *Army Munitions Survivability Program*, 1-3.

110. Rossi, *Army Munitions Survivability Program*, 1.

timelines.¹¹¹ Placing most of the US logistics capacity, including munitions handlers and cargo transfer companies, in a reserve status creates complications for the US military. Combat forces can prepare for mobilization quickly, but delays may occur because of force projection issues.¹¹²

An examination of mobilization timelines suggests the Army needs quicker and more agile response capabilities.¹¹³ Faster response would be made possible by placing more logistics assets in the active-duty Army or rapidly preparing the reserves.¹¹⁴ Logistics are important at the beginning of a conflict because forces and their munitions must be quickly projected into the theater of operations. Precious time is wasted waiting for logistics preparation to occur. If the logistics capabilities are ready at the onset of a crisis and function smoothly, the whole process can occur much more seamlessly than the speed at which the US military currently conducts business. Recovery from an attack would happen much more quickly if more logistics capabilities were in the active-duty Army or reserve logistics forces could mobilize in days.¹¹⁵

The best way to develop tactics, techniques, and procedures for mobilizing rapidly is to conduct exercises.¹¹⁶ Recently, less emphasis has been placed on logistics, even though US military leadership understands a robust logistics capability makes the United States a superpower and distinguishes it from its rivals. With most logistics capability now in the reserves, a reevaluation of the mobilization of US forces is necessary. The US Army Reserve has proposed changes to its mobilization timelines: “To provide this significant surge capacity to counter full-spectrum threats, the USAR is now focused on developing 25,000 to 33,000 soldiers in key enabling units it calls ‘Ready Force X’ that can deploy to the fight in a matter of days and weeks.” The Ready Force X concept would go a long way in resolving the logistics mobilization problem currently facing the US military.¹¹⁷

The US military’s training exercises and logistics ROC drills are not as effective as they should be. Rotations going to Europe offer prime opportunities to deploy forces and gain valuable lessons learned.¹¹⁸ The exercises never assume a contested environment and skip or waive the logistics buildup portions of the training. Logistics training exercises or ROC drills could draw more attention to the issue and provide a greater understanding of the resources required for a quick recovery.

111. Joseph Whitlock, “The Army’s Mobilization Problem,” *War Room* (blog), October 13, 2017, <https://warroom.armywarcollege.edu/articles/armys-mobilization-problem/>.

112. Whitlock, “Army’s Mobilization Problem.”

113. Whitlock, “Army’s Mobilization Problem.”

114. Whitlock, “Army’s Mobilization Problem.”

115. Whitlock, “Army’s Mobilization Problem,” 1.

116. Kurt J. Ryan, “Power Projection Readiness: A Historical Perspective,” *Army Sustainment* 49, no. 3 (May–June 2017): 27.

117. Whitlock, “Army’s Mobilization Problem.”

118. Ryan, “Power Projection Readiness.”

Could allies and partners assist the United States if it were attacked? Attacking the US munitions storage and distribution network could destroy essential stocks. The United States may need the support and assistance of allies and partners if the munitions infrastructure is attacked. Multinational training in logistics and the standardization of weapons and munitions across NATO and other alliances should be a primary goal for the US government and NATO.¹¹⁹ In addition, multinational exercises that stress logistics, including munitions logistics, should be conducted.¹²⁰ The NATO alliance has not dedicated enough resources to developing logistics interoperability.¹²¹ Furthermore, NATO should value interoperability and redundancy more to make the alliance more resilient to attack.

If the United States were attacked and Article 5 of the North Atlantic Treaty were invoked, the nation would be able to recover and respond more quickly with the support of interoperable allies. Standardization and interoperability are essential, and many leaders within the military do not appreciate that munitions, in many cases, are produced specifically for a single country's weapons. For example, during the Persian Gulf War, "the small-arms purchases from our allies did not go well. Ammunition procured from the United Kingdom performed to NATO standards in our weapons, but a difference in propellant mixes quickly fouled those weapons. The Department of the Army quickly directed that United Kingdom ammunition would not be allowed into combat areas and would only be designated as training ammunition."¹²² The same issue could affect the US military and its allies if the goal of achieving interoperability fails. Munitions interoperability would likely reduce tensions in warfare significantly and increase US resiliency.

CONCLUSION

When viewed in isolation, many of the resource cuts and streamlining that have occurred by following a business model that stresses efficiency in the maintenance of munitions logistics infrastructure have made sense. Making military reductions at a time when the Soviet Union had collapsed and no near-peer adversary existed was the prudent course to follow. Cashing in on a peace dividend seemed to be the best course and in the best interest of the American people at the time. But the power balance in the world is shifting, and new and growing threats are emerging. The US military must defend against these threats. Though the United States is working diligently to protect and prevent attacks on its soil, a near-peer adversary could breach the nation's preventative and protective measures. The combined effects of the entire logistics infrastructure that enables force projection need to be studied. Locating choke points and overcoming them are essential to ensure a seamless flow of supplies. The erosion of the industrial base, cuts in the workforce (placing most logistics in the reserves with slow mobilization timelines), and a dwindling supply of

119. Christie, "Multinational Logistics Interoperability," 14.

120. Christie, "Multinational Logistics Interoperability."

121. Christie, "Multinational Logistics Interoperability."

122. Schorr and Deal, "Ammunition Management."

US Merchant Marine ships have put the United States in a precarious position. Collective resource cuts across the services have created single points of failure that would make recovering from an attack on the US munitions infrastructure—especially Military Ocean Terminal Sunny Point or Military Ocean Terminal Concord—very difficult.

5. THE INTERSTATE HIGHWAY SYSTEM: REINVESTMENT NEEDED

Established in the late 1950s, the Dwight D. Eisenhower National System of Interstate and Defense Highways, also known as the Interstate Highway System, is one of the greatest public-works projects in US history. The system has made travel faster, easier, and safer.¹ The system has also significantly enhanced the US economy and is “the engine that has driven America’s industrial growth.”² By 1979, the final section of Interstate 5 connected Canada and Mexico.³ In 1990–91, the system contributed significantly to the success of Operation Desert Storm. “The US Highway System supported the mobilization of troops and moved equipment and forces to embarkment ports—this was key to the successful deployment.”⁴ The system has facilitated commerce exponentially, boosting the US economy by trillions of dollars. For example, US gross domestic product rose from \$426 billion in 1955, the year before the Federal Aid Highway Act authorized the system’s creation, to \$18,745 billion in 2016.⁵

The 2017 *National Security Strategy* lists “promote American prosperity” as one of four vital national interests.⁶ Subsequently, the strategy underscores the need for federal, state, and local governments to work with private industry to improve the nation’s infrastructure.⁷ While facilitating significant economic growth, the Interstate Highway System has simultaneously saved hundreds of thousands of lives by improving safety with wider lanes, uniform standards, and universal signage and numbering. As of 1996, the system was credited with saving at least 187,000 lives.⁸ Its significant contributions to the US economy, the source of US power, as well as its vulnerabilities justify designating the conditions of the Interstate Highway System a national security issue.

Title 32 of the US Code states, “it shall be policy of the DOD to integrate the highway needs of the national defense into the civil highway programs of the various state and federal agencies and cooperate with those agencies in matters pertaining to

1. Elisheva Blas, “The Dwight D. Eisenhower National System of Interstate and Defense Highways: The Road to Success?,” *History Teacher* 44, no. 1 (November 2010): 1.

2. Tim Minahan, “Interstate Highways Pay Off,” *Purchasing* 121, no. 3 (September 5, 1996): 45.

3. Doug Briggs, “USTRANSCOM JDPAC/SDDC TEA” (PowerPoint presentation, 2018 Committee on Transportation System Operations Annual Meeting, Atlanta, GA, August 27–29, 2018), 17.

4. Briggs, “USTRANSCOM JDPAC/SDDC TEA.”

5. Kimberly Amadeo, “US GDP by Year Compared to Recessions and Events,” Balance, updated April 28, 2021, <https://www.thebalance.com/us-gdp-by-year-3305543>.

6. Donald Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), 3.

7. Michael Gordon, “Trump Plans Shift to US Security Strategy,” *Wall Street Journal*, December 18, 2017, A1.

8. Wendell Cox and Jean Love, *The Best Investment a Nation Ever Made: A Tribute to the Dwight D. Eisenhower System of Interstate and Defense Highways* (Washington, DC: American Highway Users Alliance, June 1996), 2.

the use of public highways and in planning their development and construction.”⁹ To date, adversaries have not interfered with US military deployments from the homeland to a theater of conflict.¹⁰ The US military uses the Interstate Highway System in peacetime and during conflicts to move to ports to deploy without concern over adversarial actions during deployment. But the military may no longer be able to do so uncontested. “The security we have historically enjoyed between two oceans and with well-meaning neighbors to our north and south can no longer be relied upon.”¹¹ Adversaries of the United States have demonstrated capabilities that project reach to the homeland and the motivation to change the American way of war, which is to deploy unopposed and fight outside the continental United States. Consequently, “[i]t is now undeniable that the homeland is no longer a sanctuary” and must be protected.¹²

Our forces’ ability to deploy is even more critical today, after the decision was made in the mid-2000s to base the US Army primarily in the continental United States.¹³ If the United States no longer has enough forward-deployed servicemembers, it must have the ability to deploy the military quickly to the fight. This chapter discusses President Eisenhower’s original intent for the Interstate Highway System, its current status, and the actions the US government must take to ensure the effective use of the system in a contested deployment scenario. The chapter also outlines two vulnerabilities: sabotage activities in the gray zone (aggression short of armed conflict) by a state adversary and potential terrorist actions by a lone wolf or terrorist cell. The chapter recommends the US government assess and appropriate focused resources to reverse the declining condition of the Interstate Highway System, especially the interstate highway strategic connectors that connect forts to ports, and take moderate, proactive security measures to secure the system for use in a contested deployment. The chapter concludes with additional recommendations for preparing the system for use in a contested deployment.

9. “Highways for National Defense,” Transportation Engineering Agency (TEA) (website), n.d., <https://www.sddc.army.mil/sites/TEA/Functions/SpecialAssistant/Pages/HighwaysNationalDefense.aspx>.

10. Bryan Frederick et al., *Understanding the Deterrent Impact of US Overseas Forces* (Santa Monica, CA: RAND Corporation, 2020).

11. Bert Tussing and Barret Parker, “The Multi-Domain Battle: What’s in It for the Homeland?,” *War Room* (blog), November 10, 2017, <https://warroom.armywarcollege.edu/articles/multi-domain-battle-whats-homeland/>.

12. James Mattis, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: Department of Defense, January 2018), 3.

13. Carter Hamm, “A US-Based Army Can’t Get to the Fight Fast Enough,” *Defense One* (website), March 3, 2017, <https://www.defenseone.com/ideas/2017/03/us-based-army-cant-get-fight-fast-enough/135872/>.

BACKGROUND OF THE INTERSTATE HIGHWAY SYSTEM

President Eisenhower wanted to make the Interstate Highway System a reality.¹⁴ Two events in his life prior to his presidency solidified this motivation. The first event was a cross-country trip he took in 1919 when he had joined the first Army Cross-Country Motor Transport Train, which set out to learn how motor vehicles could cross the country.¹⁵ The convoy averaged about five miles per hour, had many breakdowns, and took 56 days to complete the trip. The train ride was Eisenhower's first involvement with US roads.¹⁶ The second event that impressed him happened during his service in Germany during World War II, when he saw the wide, four-lane roads built across that country for its military transport. Years later, after he was elected president, the United States still clearly needed a highway system. In addition, Eisenhower wanted the highways as part of his overall Cold War program—to be available for the evacuation of major cities in a nuclear-attack scenario and to help facilitate US military movement across the country.¹⁷

According to *The Best Investment a Nation Ever Made*, "On June 29, 1956, President Eisenhower signed the Federal Aid Highway Act of 1956 which authorized the interstate highway system."¹⁸ The federal government paid for the construction of most of the highway system, leaving a small portion for the states to fund. "The final system was 46,876 miles long and took thirty-seven years to complete."¹⁹ The Strategic Highway Network (STRAHNET) includes 1,700 miles of highways called STRAHNET Connectors that link military installations and ports.²⁰ Federal and state governments—unlike much of the nation's infrastructure, which is privately owned—own the Interstate Highway System and have standardized road features such as signage, dimensions, and numbering.²¹ These measures have led to increased commerce and travel and improved safety. The Federal Aid Highway Act also established the Highway Trust Fund, which levies taxes on gasoline and tires to finance the Interstate Highway System. The system impacts everyday life and serves as a catalyst for US economic power. The system also serves to forward deploy military forces and move forces within US borders for domestic operations. According to Mary A. Field, "Freedom of access and use of the highway system remains

14. Stephen E. Ambrose, *Eisenhower: The President*, vol. 2 (New York: Simon & Schuster, 1984), 250..

15. Blas, "Dwight D. Eisenhower National System," 128.

16. Briggs, "USTRANSCOM JDPAC/SDDC TEA," 16.

17. Ambrose, *Eisenhower*, vol. 2, 250.

18. Cox and Love, *Best Investment*, 4.

19. Blas, "Dwight D. Eisenhower National System."

20. Federal Highway Administration (FHWA) and Federal Transit Administration, *2004 Status of the Nation's Highways, Bridges, and Transit: Conditions & Performance* (Washington, DC: Department of Transportation, February 16, 2006), 18-2.

21. "Interstate Frequently Asked Questions," FHWA (website, updated April 27, 2021, <https://www.fhwa.dot.gov/interstate/faq.cfm>).

consistent with the underlying principles of democracy in the US.”²² Consequently, the Department of Homeland Security (DHS) and the Department of Transportation designated the Highway and Motor Carrier subsector as one of seven subsectors under the Transportation Systems Sector, which is one of the 16 Critical Infrastructure Sectors.²³

USE OF THE INTERSTATE HIGHWAY SYSTEM TODAY

The role of the Interstate Highway System in a deployment, contested or uncontested, has not changed much; the system is an effective medium for getting military equipment to an airport or port of debarkation.²⁴ Whether to use rail or highways to transport equipment to ports is often a cost-benefit decision.²⁵ Usually, equipment moves via highway from military installations such as Fort Bragg, North Carolina, and Joint Base Lewis-McChord, Washington, that are near a port.

The Interstate Highway System is also used to transport assets, such as US Army National Guard units responding to a domestic crisis, within the continental United States. But, the combination of organic semitrailer availability for military units and size and weight limits of vehicles on state highways is a limiting factor.²⁶ The Transportation Engineering Agency within Military Surface Deployment and Distribution Command maintains the data on equipment weight to make these strategic deployment decisions.²⁷

Shipping equipment via boat also remains a cost-effective means of moving equipment from the continental United States to any theater. Hence, in its *Port Look 2008* study for Congress, Military Surface Deployment and Distribution Command recommended if a shipping port is going to be designated a strategic port, its terminal access location must be within 10 miles of the Interstate Highway System.²⁸ Hence, the highway routes to the 22 (five military and 17 commercial)

22. Mary A. Field, “Highway Security and Terrorism,” *Review of Policy Research* 21, no. 3 (May 2004).

23. “Transportation Systems Sector,” Cybersecurity & Infrastructure Security Agency (website), n.d., <https://www.cisa.gov/transportation-systems-sector>.

24. Burt R. Lindsay, *Federal Evacuation Policy: Issues for Congress*, RL34745 (Washington, DC: Congressional Research Service, January 18, 2011), 1.

25. Department of Transportation Maritime Administration, *Report to Congress on the Performance of Ports and the Intermodal System* (Washington, DC: Department of Transportation, June 2005).

26. TEA, *Deployment Planning Guide*, SDDCTEA Pamphlet 700-5 (Scott Air Force Base, IL: Military Surface Deployment and Distribution Command, December 2011), 8.

27. TEA, *Deployment Planning Guide*.

28. David McClean, “SDDC Port Look Study 2008” (PowerPoint presentation, Strategic Ports Workshop, American Association of Port Authorities, March 23, 2009), 24, <https://aapa.files.cms-plus.com/SeminarPresentations/2009Seminars/09OpsSafetyIT/Jungwaelter.pdf>.

strategic seaports that move military equipment are publicly known and could potentially be targeted.²⁹

A present-day attack on the Interstate Highway System would certainly disrupt a military deployment. At a minimum, such an attack would slow the progress of a unit traveling to the port of debarkation. The threat of an attack would cause the unit to posture in a higher-security status and would dictate additional security actions. For example, more soldiers would be performing security, which would pull manpower away from the tasks of deploying the unit. As another example, a deploying brigade combat team may require one of its infantry companies to perform security while the main body deploys.

Current Condition of US Roads and Bridges

According to Mark S. Kuhar, “As the US Interstate Highway System turns 60 years old, it faces increasing congestion, unprecedented levels of travel—particularly by large trucks—and insufficient funding to make needed repairs.”³⁰ Since 1998, the American Society of Civil Engineers has conducted a comprehensive assessment of the nation’s infrastructure every four years. When the assessment is complete, the society issues the *Report Card for America’s Infrastructure*, dividing infrastructure into categories and grading each on a scale of “A” to “F.”

In 1988, Congress chartered a report on US infrastructure by the National Council on Public Works Improvement, but, after 1988, the federal government discontinued the report. As a result, the American Society of Civil Engineers started publishing its report in 1998. The 2021 report card’s overall grade for US infrastructure is a “C-,” which is a marginal improvement over the 2017 grade of “D+.”³¹ Despite the most recent uptick, the overall grade given to US infrastructure has been trending downward since 1988, when the National Council on Public Works Improvement gave infrastructure a “C” because the reinvestments needed each year have not been made.³² According to the 2021 report card, state and local maintenance budgets have also ignored ridership growth.³³ As of 2016, Americans were driving more, and “vehicle miles travelled [was] at its second highest-ever level, second only to 2007.”³⁴

The report card’s grades for US roads have not changed much since 1998. As Americans continue to drive more, roads have become more congested, and their

29. “Ports for National Defense,” TEA (website), n.d., <https://www.sddc.army.mil/sites/TEA/Functions/SpecialAssistant/Pages/PortsNationalDefense.aspx>.

30. Mark S. Kuhar, “Interstate Highway System Turns 60,” *Rock Products* 119, no. 7 (July 2016): 88.

31. American Society of Civil Engineers (ASCE), *2021 Report Card for America’s Infrastructure: A Comprehensive Assessment of America’s Infrastructure* (Reston, VA: ASCE, March 3, 2021).

32. “Report Card History,” American Society of Civil Engineers’ 2021 Infrastructure Report Card, 2021, <https://infrastructurereportcard.org/making-the-grade/report-card-history/>.

33. ASCE, *2017 Infrastructure Report Card: A Comprehensive Assessment of America’s Infrastructure* (Reston, VA: ASCE, March 9, 2017).

34. ASCE, *2017 Infrastructure Report Card*.

condition continues to deteriorate. In 2014, drivers spent 6.9 billion hours in traffic delays (42 hours per driver) on the four million miles of US roads, which translates into approximately \$160 billion wasted in time and fuel.³⁵ The 2017 report card also states the backlog of highway and bridge capital needs totaled \$836 billion, \$420 billion of which represented needed repairs.³⁶ In 2015, President Obama signed the Fixing America's Surface Transportation Act, which provided \$305 billion for fiscal years 2016–20 for surface transportation programs, including federal highways.³⁷ The federal government remains the major funding source for new highway construction through the Highway Trust Fund, and states are responsible for the operations and maintenance of all highways except those on federal lands.³⁸ The Highway Trust Fund, which represents the bulk of federal investment in the Interstate Highway System and is funded by use-tax revenue, teeters on insolvency, mostly because per-gallon gasoline taxes have not increased since 1993.³⁹ The taxes of 18.4 cents per gallon of gasoline and 24.4 cents per gallon of diesel have not been raised since 1993, and inflation has cut its purchasing power by 40 percent.⁴⁰

Bridges scored better than roads on the 2017 *Infrastructure Report Card* because local, state, and federal governments have made a focused, funded effort to repair structurally deficient bridges—defined as bridges that require replacement or significant maintenance. But, of the nation's 614,387 bridges, 9.1 percent, down from 12.3 percent in 2007, remain structurally deficient, almost 40 percent are 50 years or older, and the maintenance backlog for bridges totals \$123 billion.⁴¹

The report card's recommendations for roads and bridges include an increase in funding at all levels of government to improve the condition of the Interstate Highway System. In addition, the report card recommends the US government raise the federal motor fuels tax and index it to inflation to sustain the Highway Trust Fund, prioritize maintenance to maximize road and bridge life span, and tackle congestion with an optimized, multimodal transportation system for crowded metropolitan areas. Furthermore, the report card recommends builders use newly innovative materials, building technologies, and techniques to enable them to make bridges more effectively and efficiently. Road design, planning models, and new materials have improved, making roads more sustainable.⁴² For example, sensors on bridges provide feedback on

35. ASCE, 2017 *Infrastructure Report Card*.

36. ASCE, 2017 *Infrastructure Report Card*.

37. "A Summary of Highway Provisions," FHWA (website), updated February 8, 2017, <https://www.fhwa.dot.gov/fastact/summary.cfm>.

38. ASCE, 2017 *Infrastructure Report Card*.

39. Tax Policy Center, *Tax Policy Center Briefing Book* (Washington, DC: Urban Institute and Brookings Institution, 2020), 445.

40. ASCE, 2017 *Infrastructure Report Card*, 78.

41. ASCE, 2017 *Infrastructure Report Card*.

42. ASCE, 2017 *Infrastructure Report Card*, 30.

conditions, enabling engineers to address issues sooner.⁴³ Also, the National Guard's DHS vulnerability assessment teams could be used to conduct assessments on the 2,000 miles of STRAHNET Connectors used for deployments.

Interstate Highway System Vulnerabilities

Besides its deteriorating condition, the Interstate Highway System has several vulnerabilities. These vulnerabilities include being open to subversive actions in the gray zone by adversaries as well as terrorist acts.⁴⁴ The author acknowledges some of the Interstate Highway System's most serious vulnerabilities include various types of cyberattacks, such as those that disable streetlights or disrupt traffic flow. The focus here is on deliberate, physical acts perpetrated on the Interstate Highway System. For the purposes of this chapter, "physical vulnerabilities" are vulnerabilities that could result in human casualties, damage to equipment, or damage to tangible infrastructure. Examples provided later will examine two Interstate Highway System vulnerabilities exploited by ill-intentioned actors who executed deliberate, planned acts to disrupt a US military deployment, cause casualties, or destroy property.

Gray-Zone Activities

According to Charles R. Burnett et al., "[T]he gray zone is a broad carrier concept for a universe of often-dissimilar strategic challenges" between traditional war and peace.⁴⁵ State and nonstate actors with ill intentions operate in this space. Gray-zone activities occur below the threshold contained in Article 5 of the North Atlantic Treaty and below the level of violence needed to call for a UN Security Council resolution.⁴⁶ Russia's recent gray-zone activities have triggered adverse US and Western responses, including economic sanctions, but these transgressions remain well below the West's vague threshold of provocation.⁴⁷ Activities in the gray zone cause instabilities and can disrupt and delay US deployments. Like many other pieces of infrastructure, the Interstate Highway System remains vulnerable to gray-zone activities. Burnett et al. state, "The gray zone also includes the less purposeful and more incidental confluence of destabilizing, competitive forces."⁴⁸ Given the Interstate Highway System's current, poor condition, the system is even more vulnerable to gray-zone activity.

State actors do not need to be near the United States to engage in gray-zone activities. Few resources are required for an actor to operate in the gray zone, and the gray

43. ASCE, *2017 Infrastructure Report Card*, 29.

44. Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for US Military Strategy* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2016), 41.

45. Charles R. Burnett et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2016), xiii.

46. Echevarria, *Operating in the Gray Zone*, 12.

47. Burnett et al., *Outplayed*, 41.

48. Burnett et al., *Outplayed*, 10.

zone limits the actor's exposure, thereby maintaining the ability for denial. An adversary would probably rely heavily on social media and cyber warfare to conduct gray-zone activities against the United States. Some examples of potential adversarial, gray-zone activities include spreading disinformation to incite protests or strikes and disseminating lies about road conditions to delay a deployment. Russia spread disinformation before the 2016 presidential election: "Russian operatives used Facebook to publicize 129 phony event announcements during the 2016 presidential campaign, drawing the attention of nearly 340,000 users—many of whom said they were planning to attend" these phony events.⁴⁹ At a minimum, gray-zone activities cause the target to spend valuable resources in addressing the incident, but the activities stop short of defeating the target—at least, in the traditional sense. In the case of the Interstate Highway System, gray-zone activities could cause delays, prompting the United States to spend more resources during mobilization. The additional resources could be funding, such as spending money to repair a stretch of road; personnel, such as deploying soldiers to secure a stretch of interstate; or time, such as spending time navigating obstacles on the way to a port of debarkation.

One possible scenario is an adversary using gray-zone operations to delay and disrupt a deployment of US forces to the adversary's theater. China, Iran, and Russia regularly operate in the gray zone.⁵⁰ Russia, in particular, channels its gray-zone activities toward the vulnerabilities of its adversaries.⁵¹ Russia has made gray-zone activities part of its doctrine, as exemplified by its Gerasimov model or doctrine (named after Chief of the General Staff of the Russian Armed Forces Valery Gerasimov), which is a veritable playbook for gray-zone competition and conflict.⁵² Russia has demonstrated gray-zone capabilities in Crimea and eastern Ukraine, where it sent Russian journalists before invading the region to provide a pro-Russian media slant during the invasion. Russia also repaired railways in Ukraine before the invasion under the guise of humanitarian assistance and later used these railways to move troops and equipment.⁵³

Hypothetically, an adversary could destroy US private satellites, which control navigational tools many interstate travelers rely on and which companies use to track over-the-road shipments. Military systems also rely significantly on satellites.⁵⁴ Many military systems could be disabled before US forces deploy overseas,

49. Craig Timberg and Elizabeth Dwoskin, "Russians Got Tens of Thousands of Americans to RSVP for Their Phony Political Events on Facebook," *Washington Post* (website), January 25, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/01/25/russians-got-tens-of-thousands-of-americans-to-rsvp-for-their-phony-political-events-on-facebook/?utm_term=.717b9a2118e8.

50. Burnett et al., *Outplayed*, 29.

51. Burnett et al., *Outplayed*.

52. Burnett et al., *Outplayed*, 44.

53. Burnett et al., *Outplayed*.

54. "The BBC Asks What Would Happen If All Satellites Stopped Working," Code Green Prep, (website) July 30, 2013, <https://codegreenprep.com/2013/07/the-bbc-asks-what-would-happen-if-all-satellites-stopped-working>.

preventing forces from mobilizing to the theater of conflict. Without satellites, the US military would be forced to return to methods of fighting previously used. Disinformation, another gray-zone tactic, could potentially disrupt use of the Interstate Highway System. Disinformation spread by Russia could incite protesters on and around a US interstate, cause a highway worker strike, or provoke terrorists and sympathizers to disrupt troop movements, among other potential outcomes.

Terrorism

Another Interstate Highway System vulnerability that should concern strategic planners is terrorism. Before the September 11 attacks, officials and the American public had dedicated little thought to the idea a terrorist might intentionally destroy a bridge or attack a convoy. The Transportation Security Task Force, formed post-9/11 by state transportation officials, identified explosive attacks on key infrastructure as the principal threat to the highway physical infrastructure.⁵⁵ In the early 1990s, the transportation industry shipped 800,000 daily loads of hazardous material through all US modes of transportation, with 94 percent of the loads transported by trucks, according to a 1998 study for the Department of Transportation Research and Special Programs Administration.⁵⁶ The two most predominate hazardous material products shipped by the transportation industry are chemicals and petroleum products.⁵⁷

The US government and the transportation industry executed several actions to counter an explosive attack on a piece of key infrastructure. Per President George W. Bush's Executive Order 13228, the Office of Homeland Security was charged with coordinating the efforts to protect critical infrastructure, including highways.⁵⁸ The Department of Transportation soon regulated hazardous material transportation by all modes in 2001.⁵⁹ The department requires motor carriers transporting hazardous material greater than or equal to specified amounts for commerce, both interstate and intrastate, to register their loads with the Research and Special Programs Administration.⁶⁰ States enforce this registration through roadside inspection programs. But states do not require hazardous material carriers to register in each state through which they travel.

The department does require carriers "to plan for and implement procedures to prevent unauthorized persons from taking control of or attacking hazardous material shipments."⁶¹ Stated differently, the department requires carriers to develop a security plan. Terrorists could attempt to steal the hazardous materials and

55. Field, "Highway Security and Terrorism," 317.

56. Field, "Highway Security and Terrorism," 319.

57. Field, "Highway Security and Terrorism," 320.

58. John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, RL32631 (Washington, DC: Congressional Research Service, October 1, 2004), 6.

59. Moteff and Parfomak, *Critical Infrastructure*.

60. Field, "Highway Security and Terrorism," 324.

61. Field, "Highway Security and Terrorism."

commit numerous, terrible actions with them to spread panic, such as poisoning a water reservoir or building bombs for later use. The methods at terrorists' disposal include "crashing shipments into large buildings, government installations, or historic monuments."⁶²

Terrorists have used simpler tactics involving roadways, such as driving a truck into a crowd. Data from the company Calpipe Security Bollards indicate "vehicular terror attacks in 2016 killed 601 people in Western nations—more than bombings, shootings, and stabbings combined."⁶³ For example, on October 31, 2017, Sayfullo Saipov drove a rented truck down a pedestrian bike lane in New York City, killing at least eight people.⁶⁴ In October 2010, al-Qaeda published the article "The Ultimate Mowing Machine" in its *Inspire* magazine. The article calls for using a truck as a "mowing machine, not to mow grass, but to mow down the enemies of Allah."⁶⁵ Terrorists may easily obtain inexpensive vehicles, and such an act would be consistent with calls by leaders of the Islamic State of Iraq and Syria to "use what you have on hand."⁶⁶ Terrorists could learn of a tactical movement to a port and drive a truck into an area where soldiers or marines are massing, such as a deployment staging area, tactical halt formation, or marshaling area.

Terrorists could also combine the two previously mentioned strategies to fill a truck with explosives and use it as a weapon, similar to suicide bombings overseas. According to Brian Jenkins et al., "Terrorists, notably in Iraq, have attempted to increase the lethality of their devices by adding propane tanks or toxic chemicals to them."⁶⁷ Terrorists could also disrupt troop movements by destroying a key part of the Interstate Highway System, such as a bridge, or attack state troopers or state-level transportation personnel who are responsible for providing convoy movement control on the system (when requested by the military).⁶⁸

62. Chris Kilbourne, "Safe and Sound: Hazmat Transportation Security," EHS Daily Advisor (website), January 19, 2010, <https://ehsdailyadvisor.blr.com/2010/01/safe-and-sound-hazmat-transportation-security/>.

63. Max Kutner, Beatrice Dupuy, and Christina Silva, "NYC Attack: Why ISIS and Terrorists Use Trucks to Kill People and Spread Fear," *Newsweek* (website), October 31, 2017, <http://www.newsweek.com/nyc-attack-why-isis-and-terror-groups-use-trucks-kill-innocent-people-and-698032>.

64. Fox News, "New York State Heightens Security Following Manhattan Terror Attack," Fox News, October 31, 2017, <https://www.foxnews.com/us/2017/10/31/new-york-state-heightens-security-following-manhattan-terror-attack.html>.

65. CNN Wire Staff, "New Issue of Magazine Offers Jihadists Terror Tips," CNN, October 12, 2010, <https://www.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html>.

66. Holly Yan, "Vehicles as Weapons: Melbourne Part of a Deadly Trend," CNN, December 21, 2017, <https://www.cnn.com/2017/03/22/world/vehicles-as-weapons/index.html>.

67. Brian Jenkins et al., *Potential Terrorist Uses of Highway-Borne Hazardous Materials*, MTI Report 09-03 (San Jose, CA: Mineta Transportation Institute, January 2010), 1.

68. FHWA, *Coordinating Military Deployments on Roads and Highways: A Guide for State and Local Agencies* (Washington, DC: Department of Transportation, May 2005), 10.

Currently, only five military seaports can execute large-scale military deployments.⁶⁹ Several of the military seaports are close to commercial ones. Hence, terrorists or gray-zone actors, without much difficulty, could estimate the Interstate Highway System or rail routes US forces would use to move to these five ports. For example, Military Ocean Terminal Sunny Point, the largest military terminal in the world and the place from which 90 percent of ammunition going to Iraq and Afghanistan was shipped, has only one road leading to it from Interstate 95.⁷⁰

Recommendations

To prepare for a contested deployment scenario, the United States needs to ensure the Interstate Highway System is in adequate condition and protected. Despite post-9/11 countermeasures taken to protect the Interstate Highway System, terrorists or other adversaries may still exploit it. Highways are the most difficult infrastructure to secure against threats. The National Bridge Inventory contains more than 3.9 million miles of public roads and 591,548 structures.⁷¹ The highway system connects all modes and provides a readily available and affordable means for would-be terrorists to gain access to the United States through Canada and Mexico.⁷² The protection recommendations that follow include some measures to protect all infrastructure and others to protect the STRAHNET Connectors for use in a contested deployment.

An example of a proactive infrastructure protection program is the National Association of Chemical Distributors quality control program for members who ship hazardous materials. The government should consider mandating a standardized template to be used nationally. The program could then be able executed consistently with inspections to prevent terrorists from acquiring bomb-making materials.

Another proactive program for the Interstate Highway System at large is the government's "If You See Something, Say Something" public awareness campaign, which calls for the public to report suspicious activity to local authorities. The federal government could establish a national hotline for reporting incidents that may be related to terrorism and consolidate the various state-level hotlines for reporting suspected terrorist activities. For example, New York State uses 1-866-SAFENYS,

69. FHWA, *Coordinating Military Deployments*, 13.

70. "Military Ocean Terminal Sunny Point (MOTSU)," World Port Source, n.d., https://worldport-source.com/ports/review/USA_NC_Military_Ocean_Terminal_Sunny_Point_MOTSU_3601.php.

71. Steven B. Chase and Jeffrey A. Laman, *Dynamics and Field Testing of Bridges* (Washington, DC: Transportation Research Board, January 2000).

72. Bill McGee, "Border Crossing Checklist: Tips for Road Trips to Canada and Mexico," *USA Today* (website), June 29, 2016, <https://www.usatoday.com/story/travel/columnist/mcgee/2016/0629/canada-mexico-border-crossing/86470696/>.

and New York City uses 1-888-NYCSAFE.⁷³ The federal government should establish one hotline with a memorable phone number so it becomes nationally known, similar to 911. A single hotline would also make data easier to capture and use for trend analysis. Local responders should be able to receive the information immediately, and analysts at the state and federal levels should be able to capture and review the data quickly. Billboards and signage on the Interstate Highway System could reinforce and promote the hotline, and it could be incorporated into the National Response Framework. The hotline would fit neatly into the framework's mission area of "Response—the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred."⁷⁴ The hotline would also fit into the Response core capability of Public Information and Warning: "[T]o deliver coordinated, prompt, reliable, and actionable information to the whole community."⁷⁵ These capabilities can warn the public, and the public can use them to remain vigilant for terrorist or gray-zone activities. Like the National Response Framework, the customer base for the hotline should be entire communities.

A solution should also consider using the National Guard's DHS vulnerability assessment teams to evaluate all 2,000 miles of the STRAHNET Connectors. Recommendations for improvements based on the evaluations could be made to ensure the Interstate Highway System continues to be ready for deployments. Additionally, federal and state governments should sustain maintenance budgets to at least meet annual requirements and protect them from being raided for other projects to prevent the United States from regressing into a significant backlog again.

After the Department of Defense reviews the vulnerability assessment team evaluations, it could task the National Guard with protecting the critical sections of the STRAHNET Connectors. Giving the National Guard this responsibility would reduce the requirement for deploying units to perform security-related tasks and allow them to concentrate on the many other tasks associated with deployment. Joint Task Force Empire Shield provides a possible template for this strategy: New York National Guard soldiers maintain a visible presence to deter terrorists throughout transit hubs like Grand Central Station and Penn Station in the New York City area.

National Guard soldiers in Title 32 status, when the Posse Comitatus Act does not apply, have law enforcement authorities that could be used to facilitate deployments by securing the STRAHNET Connectors and ports. These missions should be assigned to state National Guards where the critical infrastructure resides, enabling them to rehearse their responsibilities and further develop interagency relationships. For example, the Department of Defense could task the North Carolina National Guard

73. "24/7 Hotline Gathers Information from the Public about Suspected Terrorist Activity," New York State Division of Criminal Justice Services, n.d., <https://www.criminaljustice.ny.gov/tipsline.htm>.

74. Department of Homeland Security (DHS), *National Response Framework*, 2nd ed. (Washington, DC: DHS, May 2013), 1.

75. DHS, *National Response Framework*, 20.

with the responsibility of securing the route from Fort Bragg, North Carolina, to Military Ocean Terminal Sunny Point.

The National Guards within these states already possess the interagency relationships at the state and local level. These National Guards could coordinate routine interagency exercises at the state and local levels to rehearse security implementation on the Interstate Highway System. Many National Guards already conduct similar interagency training with state and local agencies for evacuation scenarios. More units, especially active-duty ones, are conducting tactical deployment exercises on their way to Combat Training Center rotations.⁷⁶ The 82nd Airborne Division announced in March 2018 it had convoyed vehicles from Fort Bragg along Interstate 95 to Joint Base Charleston, South Carolina, to be transported via boat to Fort Polk, Louisiana, for a Joint Readiness Training Center rotation.⁷⁷ “The 82nd Airborne said [it was] one of the division’s largest sealift deployment exercises in decades.”⁷⁸ Units could familiarize themselves with topics such as clearances needed for oversize loads and alternate routes during periods of congestion. Long stretches of the Interstate Highway System should be assigned a mobile yet visible security solution.

Also known as the “ring of steel,” the United Kingdom’s Traffic and Environmental Zone uses checkpoints and concrete barriers to protect civilians, an ideal technique for countering terrorists who may wish to drive a heavy vehicle into a military formation.⁷⁹ After two terror attacks occurred in London in 2017, during which terrorists driving vehicles mowed down pedestrians, antiterror measures such as checkpoints, an extended perimeter, and concrete barriers were installed in pedestrian areas in major cities like London and Manchester to prevent heavy vehicles from driving into crowds.⁸⁰ These concepts may be applied to marshaling areas at home stations, tactical pauses en route to ports of debarkation, or ports of debarkation. These measures cost very little, but units should train on the procedures that are selected and develop them into standardized operating procedures.

Finally, Congress should pass legislation providing for a focused reinvestment in critical infrastructure—especially STRAHNET Connectors, rails, and ports used for deployment. The American Recovery and Reinvestment Act of 2009 included \$83 billion to improve infrastructure, one of seven focus areas to help stimulate

76. Headquarters, Department of the Army (HQDA), *Combat Training Center Program*, Army Regulation 350-50 (Washington, DC: HQDA, May 2, 2018).

77. WLTX, “Military Convoys from North Carolina Hit Southern Highways,” WLTX, March 19, 2018, <https://www.wltx.com/article/news/local/military-convoys-from-north-carolina-hit-southern-highways/101-529618371>.

78. WLTX, “Military Convoys.”

79. Russell Myers, “Terror Attack Fears Prompt Ring of Steel around Britain’s Christmas Markets to Protect Revelers,” *Daily Mirror*, October 16, 2017, <https://www.mirror.co.uk/news/uk-news/terror-attack-fears-prompt-ring-11352601>.

80. Myers, “Terror Attack Fears.”

the economy.⁸¹ As of September 2021, proposed legislation dedicates an additional \$110 billion for “roads, bridges, and other major projects” as part of a larger \$550 billion infrastructure package.⁸² Until this bill passes, it is unknown what percentage of projects will focus on infrastructure identified by the Department of Homeland Security as critical infrastructure, but we suggest roads, bridges, ports, and airfields needed for the Department of Defense to project assets should be a priority.⁸³

The 2017 American Society of Civil Engineers report card estimates bringing US infrastructure up to a “B” grade would require spending \$4.59 trillion over 10 years. According to this report card, “The Federal Highway Administration estimates that each dollar spent on road, highway, and bridge improvements returns \$5.20 in the form of lower vehicle maintenance costs, decreased delays, reduced fuel consumption, improved safety, lower road and bridge maintenance costs, and reduced emissions.”⁸⁴

CONCLUSION

In summary, the tremendous economic and societal impacts of the Interstate Highway System over the last 65 years have revolutionized the Americans way of life. The system’s poor condition remains undeniable. Though one of the primary reasons Eisenhower built the system was military mobilization, Americans have spent little time considering this use of the system. The US armed forces have never had a contested deployment involving adversarial actions within US borders. As a result, the military seems to assume deployments will be uncontested. This assumption may no longer be valid. The Interstate Highway System has physical vulnerabilities—namely, from gray-zone actors and terrorists, each capable of disrupting and delaying deploying forces.

The Interstate Highway System, including the STRAHNET Connectors, requires substantial, focused investment and security for the military to be prepared for a contested deployment. Proactive security measures to counter the system’s vulnerabilities include making the National Association of Chemical Distributors quality control program mandatory, consolidating counterterrorism reporting hotlines, and using the National Guard in Title 32 status to provide physical security at designated bridges and STRAHNET Connectors. Most of all, like most US critical infrastructure, the Interstate Highway System needs the government to assess it and make focused reinvestment in the roads, bridges, and other pieces of infrastructure needed for the deployment of forces. These measures would protect the

81. Residential Retrofit Working Group, *Roadmap for the Home Energy Upgrade Market* (Washington, DC: State & Local Energy Efficiency Action Network, June 2011), ix, 15, 23.

82. White House, Fact Sheet: Historic Bipartisan Infrastructure Deal, July 28, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-historic-bipartisan-infrastructure-deal/>.

83. Robert Pollin and Heidi Garrett-Peltier, *The US Employment Effects of Military and Domestic Spending Priorities: 2011 Update* (Amherst, MA: Political Economy Research Institute, December 2011), 4.

84. ASCE, *2017 Infrastructure Report Card*, 77.

system and the US way of war—projecting forces from the continental United States—and fit in with President Eisenhower’s vision of “a mighty network of highways spread across the country.”⁸⁵

85. “50th Anniversary Interstate Highway System—Eisenhower Audio Gallery,” FHWA (website), updated June 27, 2017, <https://www.fhwa.dot.gov/interstate/audiogallery.cfm>.

APPENDIX A

CONTESTED DEPLOYMENT CYBER INDEX

INTRODUCTION

This appendix includes the findings of a US Army War College research team consisting of faculty and students. The team explored how Department of Defense (DoD) cyber units should respond to a cyberattack on US critical infrastructure that supports the deployment of forces from the United States and what these cyber units could do to speed the recovery of critical infrastructure systems. This research continues the efforts of the Maneuver Support Battle Lab, which published the *Contested Deployment Seminar (CDS) Event Report* on October 5, 2016. Seminar participants explored the impact of a state actor conducting anti-access operations within the United States to disrupt and delay a deployment of forces. The scenario included a major hurricane and cyberattacks on the electrical grid and deployment infrastructure. Despite these challenges, the seminar concluded the deployment system was resilient and noted only minor delays.¹ In addition, the participants found “[a] number of doctrinal and policy issues impact the use of military cyber capability in the homeland as well as potential kinetic attacks on cyber targets within the homeland. These issues would likely leave these actions in the hands of civilian authorities unless they are updated.”²

The Department of Defense has recognized it must be prepared to defend the nation’s critical infrastructure from a cyberattack, and assumed in its 2015 cyber strategy that during a conflict, “a potential adversary will seek to target US or allied critical infrastructure and military networks to gain a strategic advantage . . . and a sophisticated actor could target an industrial control system (ICS) on a public utility.”³ The strategy then states while the Department of Defense depends on private-sector critical infrastructure to conduct operations, it is unsure of the state of the cybersecurity of these systems.⁴ The department, therefore, must work with critical infrastructure owners and operators to mitigate and respond to cyberattacks.⁵ The cyber strategy directs the Department of Defense to conduct exercises with the Department of Homeland Security and the FBI to protect critical infrastructure “under partner agencies’ lead.”⁶

Following guidance in the DoD cyber strategy, US Cyber Command missions include deterring and defeating threats to critical infrastructure. In 2017, Admiral Michael S. Rogers, commander, US Cyber Command, stated, “We are particularly

1. David Nobles, *Contested Deployment Seminar (CDS) Event Report* (Fort Leonard Wood, MO: US Army Maneuver Support Center of Excellence, October 5, 2016), 4.

2. Nobles, *Contested Deployment Seminar*, 15.

3. Department of Defense (DoD), *The Department of Defense Cyber Strategy* (Washington, DC: DoD, April 2015), 2.

4. DoD, *Cyber Strategy*, 7.

5. DoD, *Cyber Strategy*, 11.

6. DoD, *Cyber Strategy*, 22.

concerned as adversaries probe and even exploit systems used by . . . critical infrastructure in the United States and abroad.”⁷ He goes on to state the command has observed cyber intrusions into critical infrastructure both in the United States and abroad. He highlighted the 2015 cyberattack against the Ukrainian electrical power grid and stated the Department of Homeland Security notified systems administrators about malware used in this attack.⁸ If these cyberattacks were directed at American critical infrastructure that supports the military, the resulting effects could hamper deployments and the command and control of US forces.⁹ US Cyber Command manages only a portion of the whole-of-nation effort required to defend US critical infrastructure. The command coordinates with the FBI and the Department of Homeland Security to protect national critical infrastructure and includes the US Army Reserve and the National Guard when responding to significant cyber incidents.¹⁰

For the past nine years, US Cyber Command has conducted annual Cyber Guard exercises to evaluate the Cyber Mission Force, other government agencies, and state organizations’ capabilities to defend critical infrastructure. During Cyber Guard 2017, over 700 government and critical infrastructure cybersecurity experts coordinated efforts to respond to a variety of cyber threats. The Cyber Mission Force supported the Department of Homeland Security in helping a private-sector organization recover from a cyberattack on the electrical grid. National Guard cyber teams responded in their Title 32 role, testing the dual-status command concept in this complex technical and policy environment.¹¹ With the Contested Deployment Seminar having effectively explored the cyber vulnerabilities and resiliency of the deployment system and the Cyber Guard exercises having evaluated cyber team responses, the US Army War College team authored a series of research papers to address the following questions.

- CAN: Do DoD cyber units have the capability to assist private-sector critical infrastructure organizations?
- MAY: Do current laws and policies permit DoD cyber units to assist private-sector critical infrastructure organizations?
- WHAT: What should critical infrastructure owners and operators do to enhance their cybersecurity?
- HOW: If DoD cyber units are directed to assist private-sector critical infrastructure organizations, who will command and control these units?

7. *United States Cyber Command*, 115th Cong. (2017) (statement of Michael S. Rogers, commander, US Cyber Command).

8. *United States Cyber Command*.

9. *Fiscal Year 2017 Budget Request for US Cyber Command: Preparing for Operations in the Cyber Domain*, 114th Cong. (2016) (statement of Michael S. Rogers, commander, US Cyber Command).

10. *United States Cyber Command*.

11. United States Cyber Command, “Teams Defend against Simulated Attacks in Cyber Guard Exercise,” DoD (website), July 5, 2017, <https://www.defense.gov/News/Article/Article/1237898/>.

Lieutenant Colonel Christian A. Haffey begins the appendix section by addressing the CAN question with his part titled, "Critical Infrastructure: Are Cyber Mission Forces Equipped to Defend?" This part of the appendix is not included in this integrated research project because it is classified. He examines the ability of the Cyber Mission Force, including National Guard units, to defend critical infrastructure that supports the deployment of forces from a US home station to its port of embarkation. He then explores DoD cyberspace training to determine whether Cyber Mission Force teams have the sufficient skills and resources to help public and private-sector critical infrastructure organizations defend against and recover from a cyberattack.

Haffey shows the defense of critical infrastructure requires DoD cyber teams that possess a high level of expertise in the cybersecurity of traditional information technology (IT) and operational technology, including supervisory control and data acquisition systems. He proposes the Department of Defense assess the Cyber Mission Force to determine the appropriate force structure and required team composition. He recommends US Cyber Command standardize critical infrastructure training and equipment. Teams within the Cyber Mission Force should continue to enhance their expertise through exercises that integrate government, academia, and public and private-sector cybersecurity professionals.

Next, in "Cyberspace Defense of Critical Infrastructure: Legal and Policy Limitations," Lieutenant Colonel Jonathan M. Boling addresses the MAY question. He explores legal and policy issues for DoD cyber assistance to private-sector organizations and provides an overview of the development of national cybersecurity policy and authority and policy recommendations to enable better public-private collaboration. Better interaction would allow stakeholders to prepare for, and respond to, cyber crises on public and private-sector critical infrastructure. He analyzes the Defense Critical Infrastructure Program, which "consists of actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets."¹² He further reviews the laws, policies, and regulations that apply to defense support of civil authorities and applies these standards to DoD support of critical infrastructure owned and operated by the private sector. His findings support the statement by General Keith B. Alexander, US Army retired, to Congress that clear authorities and rules of engagement are necessary to respond to cyberattacks on critical infrastructure.¹³

Boling proposes a national cyber defense plan that focuses on critical infrastructure protection. He recommends Cyber Mission Force National Mission Teams receive training and certification on the nation's most important critical infrastructure through partnerships with public and private infrastructure owners and operators. He then states many National Guard cyber team members are uniquely qualified for these tasks because their civilian positions often involve the protection of private-sector operational technology. The Department of Defense should take advantage of this opportunity to enhance National Guard

12. "Defense Critical Infrastructure Program (DCIP)," Under Secretary of Defense for Policy (website), n.d., <https://policy.defense.gov/OUSSDP-Offices/ASD-for-Homeland-Defense-and-Global-Security/Defense-Critical-Infrastructure-Program/>.

13. *Cyber Strategy and Policy*, 115th Cong. (2017) (statement of Keith B. Alexander, chief executive officer and president, IronNet Cybersecurity).

cyber team response capabilities to cyberattacks on critical infrastructure. Boling also echoes the previous part in calling for more DoD cybersecurity exercises with governmental partners.

The next part addresses the WHAT question. Colonel Brian D. Wisniewski's, "Framework for a Critical Infrastructure Cyber Resilience Assessment," examines the processes critical infrastructure owners and operators should implement to enhance cybersecurity and attempts by China, Iran, North Korea, and Russia to gain advantage through cyberspace activities resembling Indian strategist Chanakya's concept of "silent war." Wisniewski then assesses current international standards and best practices and concludes with recommendations for improving these practices.

Wisniewski's first recommendation is for the continued support and expansion of international standards and industry best practices designed to improve cybersecurity constantly. He then proposes a framework for the cyber resilience of critical infrastructure assets beyond vulnerability assessments. Finally, he recommends the United States reestablish a critical infrastructure assessment program, with a renewed focus on both security and cyber resilience.

The appendix concludes with research and findings on HOW the Department of Defense should command and control its forces in response to a cyberattack on critical infrastructure. Colonel James L. Boling, US Army retired, and Colonel Steven E. Landis, US Army retired, provide a detailed analysis in "Command and Control of Domestic Cyber Response Operations in a Complex Catastrophe." They outline a challenging scenario in which a nation-state conducts a significant cyberattack on US critical infrastructure while the Department of Defense prepares to deploy to an overseas contingency, and they compare and contrast the response to a natural disaster and a cyberattack. This part explores whether the Department of Homeland Security's *National Cyber Incident Response Plan* is sufficient to act as the command-and-control blueprint for a synchronized US response to a major domestic cyber incident, with particular attention to DoD roles and responsibilities in defense support of civil authorities. Boling and Landis then explore show how the US government should exercise whole-of-government command and control during cyber incidents.

National, state, local, and private-sector leaders must become aware of the significant vulnerabilities to critical infrastructure. With awareness comes the requirement to enhance the cybersecurity of the systems that are essential to the survival of the United States. The Department of Defense is equally dependent on these systems to project power and support civil authorities in response to crises in the homeland.

APPENDIX A-1

CYBERSPACE DEFENSE OF CRITICAL INFRASTRUCTURE: LEGAL AND POLICY LIMITATIONS

The 2018 *National Defense Strategy* summary bleakly states the United States homeland “is no longer a sanctuary.”¹ With a few minor exceptions, the country has been free from major terrorist attacks since 2001 and from major world-power attacks on the homeland since World War II. The explosive growth of technology has infiltrated every aspect of life, including homes, businesses, and the federal government, and multiple areas of science, such as energy, neuroscience, genetics, and nanotechnology.² Much of this technology has naturally wound up in the critical infrastructures that run our world, making them more reliable, easier to maintain, cheaper, and more responsive. Unfortunately, in the race to make these improvements, the same technology advances introduce potentially high-risk vulnerabilities that enable foreign manipulation or introduce the possibility of cascading failures that would interfere with the software and mechanical operations of information technology (IT) systems to disastrous effect.

Attempts to compromise these infrastructure vulnerabilities have been well documented. At a September 2017 Industrial Control Systems Cyber Security Conference, Kaspersky Lab reported “it had detected roughly 18,000 malware samples belonging to more than 2,500 families on industrial control systems (ICS) in the first half of 2017” alone.³ Compromising cyber-enabled components of transportation, energy, or financial systems offers compelling, asymmetric advantages that could cause devastating or destructive effects on the infrastructures the components service.⁴ The cybersecurity company FireEye reported in December 2017 the detection of a complex, targeted malware specifically designed to manipulate industrial processes. Speculation suggests authorship by nation-state-level expertise, and, consistent with other Stuxnet-like attacks, this malware was intended to “prevent safety mechanisms from executing their intended function, resulting in a physical consequence.”⁵ The National Cybersecurity and Communications Integration Center, the “federal-civilian interface for sharing cyber threat indicators,” said, in 2017, it “responded to diverse incidents, conducted exercises to support operational awareness, and provided

1. James Mattis, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: Department of Defense, January 2018), 3.

2. “Big Idea: Technology Grows Exponentially,” Big Think (website), March 21, 2011, <https://bigthink.com/think-tank/big-idea-technology-grows-exponentially>.

3. Eduard Kovacs, “Thousands of Malware Variants Found on Industrial Systems: Report,” Industrial Control Systems Cyber Security Conference, September 28, 2017, <https://www.icscybersecurityconference.com/thousands-malware-variants-found-industrial-systems-report/>.

4. Kovacs, “Thousands of Malware Variants.”

5. Blake Johnson et al., “Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure,” *FireEye Threat Research Blog*, December 14, 2017, <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>.

guidance” to a variety of public and private organizations.⁶ It shared over 15,600 alerts and 3,000 indicators of compromise and received “more than 106,000 incident reports from federal and state, local, tribal, and territorial (SLTT) governments and the private sector, affecting communications, enterprise, and control systems.”⁷

Because critical infrastructures are vital to the movement of deploying forces, the Department of Defense (DoD) must understand this high-threat environment and the associated cyberspace vulnerabilities and risks. In testimony to the US Senate Committee on Armed Services in 2017, General Keith B. Alexander, US Army retired, stated the Department of Defense has the responsibility to defend the nation in cyberspace, and the private sector “controls most of the real estate in cyberspace . . . and the notion that the government might have control over, or even a constant active defensive presence on these private systems and networks, is simply not something our nation seeks today.”⁸

Although much has changed in recent years, significant legal and policy limitations remain that inhibit DoD cybersecurity resources from effectively defending the nation or responding in the event of cyberattack on DoD-dependent critical infrastructures. This part of the appendix will present a brief history of the development of cybersecurity national policy, present the current capabilities under existing authorities, and provide policy recommendations to enable better public-private collaborations to prepare for and respond to cyber crises on public and private-sector critical infrastructures.

OVERVIEW OF DEFENSE SUPPORT OF CIVIL AUTHORITIES

Policy of the Department of Defense defines Defense Support of Civil Authorities (DSCA) in the following way:

Support provided by US Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.⁹

Defense support of civil authorities, which has evolved over the years as civil-military relations have evolved, is tailored mostly to national disaster response; border security augmentation; and special-event security, such as protests or political

6. National Cybersecurity and Communications Integration Center (NCCIC), *NCCIC Year in Review 2017: Operation Cyber Guardian* (Washington, DC: NCCIC, April 2, 2018), 3.

7. NCCIC, *Operation Cyber Guardian*, 20.

8. *Cyber Strategy and Policy*, 115th Cong. (2017) (statement of Keith B. Alexander, chief executive officer and president, IronNet Cybersecurity).

9. William J. Lynn III, *Defense Support of Civil Authorities*, DoD Directive 3025.18 (Washington, DC: Under Secretary of Defense for Policy, updated March 19, 2018).

event support.¹⁰ Invoking DSCA in a crisis following a critical infrastructure event is a relatively new concept.

The complexities involving federal military personnel in domestic response to traditional crises have a long and nuanced history in the United States. For many reasons outside the scope of this part of the appendix, US civil society has an abiding “wariness of standing armies . . . rooted in the colonial experience.”¹¹ Federal law inhibits military involvement in law enforcement in the United States. There is much debate on the implementation of the Posse Comitatus Act—an 1878 law—and whether military leaders and lawyers understand its application and interpretation in today’s context. Many advocate for better-defined rules of engagement.¹²

The Department of Defense has significant resources available to assist SLTT governments during national disasters and civil unrest, and a lawful mechanism permits SLTT authorities to request federal military support and enables support at the president’s request. Authorities for traditional DSCA missions, such as domestic disaster recovery or law enforcement, at the request of local authorities or when approved by the president or secretary of defense have long been established.¹³ A national crisis following a cyberattack on domestic critical infrastructures has many similarities to traditional crises, and little reason exists to believe a model other than DSCA would be appropriate in response. The US government has a long history of evolving policies to ensure the cybersecurity of critical infrastructure against the growing terrorist and criminal cyber threat.

The concern about the vulnerabilities inherent in critical infrastructures, especially with the modern introduction of cyber-based capabilities, has been growing for more than 25 years. Former President George H. W. Bush’s 1990 National Security Directive 42 recognized the necessity for securing national security systems increasingly dependent on emergent IT capabilities to ensure their operation in crisis. The directive modernized policy from the 1980s on national security systems, recognizing the need to update the policy based on the introduction of new technology.¹⁴ Though the term “critical infrastructure” had not become popular yet, the spate of terrorist and criminal attacks in the early 1990s focused national attention on the topic.

In 1996, President William J. Clinton issued Executive Order 13010. The order established a commission that spent 15 months assessing the scope and nature of vulnerabilities inherent in the nation’s haphazard interconnection of critical

10. Lynn, *Defense Support of Civil Authorities*, 2.

11. Amos A. Jordan, William J. Taylor Jr., and Michael J. Mazarr, “The Role of the Military in the Policy Process,” in *American National Security*, 7th ed. (Baltimore: Johns Hopkins University Press, 2009), 203.

12. For more information, see Donald J. Currier, *The Posse Comitatus Act: A Harmless Relic from the Post-Reconstruction Era or a Legal Impediment to Transformation?* (Carlisle, PA: US Army War College Press, 2003); and Thomas D. Cook, *The Posse Comitatus Act: An Act in Need of a Regulatory Update* (Carlisle, PA: US Army War College Press, 2008).

13. Lynn, *Defense Support of Civil Authorities*, 3.

14. George H. W. Bush, *National Policy for the Security of National Security Telecommunications and Information Systems*, National Security Directive 42 (Washington, DC: White House, July 5, 1990).

infrastructures.¹⁵ These systems were developed, interconnected, and upgraded over time with little thought to security in general and little-to-no consideration of cyber threats.¹⁶ As a result of the commission's work, Clinton signed Presidential Decision Directive 63, *Critical Infrastructure Protection: Sector Coordinators*, in 1998. This first-of-its-kind directive began assigning responsibility for critical infrastructure protection to US government agencies. Because the directive primarily focused on infrastructures used for commerce (such as banking, manufacturing, and transportation), the National Telecommunications and Information Administration within the Department of Commerce was appointed the lead agency.¹⁷

Before the September 11 attacks, the Department of Defense primarily focused on threats outside US territorial boundaries.¹⁸ After 2001, the development of US critical infrastructure protection policy expanded, and the scope of the problem affecting critical infrastructures threatened by newly discovered terroristic threats became starkly evident. As stated by Walter Neal Anderson, "In the aftermath of 9/11, the entire US government was compelled to rethink its concepts of homeland defense (HD), homeland security (HS), and defense support of civil authorities (DSCA)."¹⁹

Two rapid developments were the creation of the Department of Homeland Security in March 2003, a new agency that would be responsible for homeland security, and the establishment of US Northern Command, a new DoD Combatant Command providing a single commander responsible for the DoD's involvement in homeland defense and DSCA response in the homeland.²⁰ The Department of Homeland Security was deemed the authority for "the prevention, preemption, and deterrence of, and defense against, aggression targeted at US territory, sovereignty, domestic population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies."²¹ Homeland defense "is the protection of US territory, domestic population and critical infrastructure against military attacks emanating from outside the United States."²² US Northern Command is tasked with support to the homeland security effort.

15. Robert T. Marsh, "Foreword," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald et al. (Cambridge, UK: Cambridge University Press, 2006), xii.

16. Marsh, "Foreword," xii.

17. William J. Clinton, *Critical Infrastructure Protection: Sector Coordinators*, Presidential Decision Directive 63 (Washington, DC: White House, May 22, 1998).

18. Walter Neal Anderson, *Introduction to Homeland Defense and Defense Support to Civil Authorities (DSCA): The Military's Role to Support and Defend*, ed. Bert B. Tussing and Robert McCreight (Boca Raton, FL: CRC Press, 2015), 39.

19. Anderson, *Introduction to Homeland Defense*, 39.

20. Anderson, *Introduction to Homeland Defense*, 39–40.

21. Peter Stinson, "Homeland Security and Homeland Defense: Flexible, Multi-Capable Agencies Best for Federal Homeland Interventions," Peter Stinson, March 3, 2004, <http://papers.peterstinson.com/2004/03/homeland-security-and-homeland-defense.html>.

22. Stinson, "Homeland Security."

Both organizations evolved to develop capabilities and frameworks to respond to natural disasters and external, conventional attacks, but crises such as Hurricane Katrina highlighted the need for better integration among homeland security, homeland defense, and DSCA activities.²³ In addition, Bush's 2003 Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, established multiple-agency responsibility over nine categories of critical infrastructures and appointed the Department of Defense as the lead agency for the defense industrial base.

The directive lists the Critical Infrastructure Sectors as "[i]nformation technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping." Sector-specific federal agencies are defined as follows:

- Department of Agriculture – agriculture, food (meat, poultry, egg products);
- Health and Human Services – public health, healthcare, and food (other than meat, poultry, egg products);
- Environmental Protection Agency – drinking water and water treatment systems;
- Department of Energy – energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear-power facilities;
- Department of the Treasury – banking and finance;
- Department of the Interior – national monuments and icons; and
- Department of Defense – defense industrial base.²⁴

The directive resulted in the Department of Homeland Security *National Infrastructure Protection Plan* in 2006, which was revised in 2009 and 2013. In 2013, Bush's directive was superseded by President Barack Obama's Presidential Policy Directive 21 (PPD-21), which established a more robust framework for organizing federal and SLTT government collaboration with private-sector entities for critical infrastructure protection. The directive paired with Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, by directing the executive branch to "develop a technology-neutral cybersecurity framework, promote . . . the adoption of cybersecurity practices, increase . . . cyber threat information sharing, incorporate . . . privacy and civil liberties protections, and explore . . . existing regulation to promote cybersecurity."²⁵ The

23. Anderson, *Introduction to Homeland Defense*, 47–49.

24. George W. Bush, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (Washington, DC: White House, December 17, 2003).

25. Department of Homeland Security (DHS), "Executive Order 13636 and Presidential Policy Directive 21 Fact Sheet," United States Department of Agriculture Departmental Management, March 12, 2013, <https://www.dm.usda.gov/ohsec/nsps/EO-13636-PPD-21-Fact-Sheet.pdf>.

list of Critical Infrastructure Sectors grew to 16, with each assigned a lead federal agency, as seen in table A-1.²⁶

Table A-1. Critical infrastructure sectors and the corresponding lead federal agencies

Critical Infrastructure Sectors	Lead Federal Agency
1. Chemical	Department of Homeland Security
2. Commercial Facilities	Department of Homeland Security
3. Communications	Department of Homeland Security
4. Critical Manufacturing	Department of Homeland Security
5. Dams	Department of Homeland Security
6. Defense Industrial Base	Department of Defense
7. Emergency Services	Department of Homeland Security
8. Energy	Department of Energy
9. Financial Services Sector	Department of Treasury
10. Food and Agriculture	Department of Agriculture and Department of Health and Human Services
11. Government Facilities	Department of Homeland Security and General Services Administration
12. Healthcare and Public Health	Department of Health and Human Services
13. Information Technology	Department of Homeland Security
14. Nuclear Reactors, Materials, and Waste	Department of Homeland Security
15. Transportation Systems	Department of Homeland Security and Department of Transportation
16. Water and Wastewater Systems	Environmental Protection Agency

In 2016, following the public reporting on the Democratic National Committee e-mail hack, Obama signed PPD-41. This directive and its associated plans formalized a scale of severity for cyber incidents from zero to five (“inconsequential” to “imminent threat to national security”) and assigned investigative responsibility to the Department of Justice, the Department of Homeland Security (lead for asset protection), and the Office of the Director of National Intelligence (lead for intelligence support).²⁷ The directive also appointed the National Security Council’s Cyber Response Group to author national policy objectives and established an entity to coordinate the national, interagency operational activities through a Cyber Unified Coordination Group.²⁸

26. “Critical Infrastructure Sectors,” Cybersecurity & Infrastructure Security Agency (website), n.d., <https://www.cisa.gov/critical-infrastructure-sectors>.

27. Frank J. Cilluffo and Sharon L. Cardash, “Overview and Analysis of PPD-41: US Cyber Incident Coordination,” *Lawfare* (blog), July 27, 2016, <https://www.lawfareblog.com/overview-and-analysis-ppd-41-us-cyber-incident-coordination>.

28. Cilluffo and Cardash, “Overview and Analysis.”

The most recent executive action to address the cybersecurity of critical infrastructure was Executive Order 13800, which built on the previous administration's PPD-21 and Executive Order 13636. Executive Order 13800 directs federal agency heads to identify and prioritize cybersecurity preparations for the sectors determined "to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."²⁹ Executive Order 13800 directed a report from the secretary of homeland security on findings and recommendations.³⁰ Media reporting indicated the federal government's response to the executive order was slow. *WIRED* quoted a National Security Council official as saying, "Departments and agencies continue implementing Cybersecurity Executive Order 13800 and have made significant progress. While they continue to work toward the deadlines outlined in the Executive Order, the release of products may vary over time. However, many of the deliverables will be used to inform work going forward."³¹

Congress drafted a requirement to incorporate a national cyber policy into the National Defense Authorization Act for Fiscal Year 2018. President Trump objected to this provision, but he ultimately signed the act with the requirement intact.³² The National Cyber Strategy of the United States of America was published in September 2018.³³

CURRENT DSCA POLICIES REGARDING CYBERSPACE SUPPORT

In the event of a crisis, the Department of Defense provides support to SLTT governments or other federal agencies at their request or at the direction of the president. Recent developments in cybersecurity and the growth of DoD capabilities in cyberspace demonstrate a new capability that may prove useful during a cyberattack on the homeland. As a result, in 2016 and 2017, the deputy secretary of defense released two memoranda to provide an avenue, under existing DSCA authority, for facilitating the provision of DoD cyber expertise when requested by civil authorities or at presidential direction. The first—Deputy Secretary of Defense Policy Memorandum 16-002, *Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities*—outlines authority to "coordinate, train, advise and assist (CTAA) cyber support and services provided incidental to military training to organizations and activities outside the Department of Defense and for

29. Executive Order No. 13,800, 3 C.F.R. 22391–22397 (2017).

30. Trump, *Cybersecurity of Federal Networks*.

31. Lily Hay Newman, "Taking Stock of Trump's Cybersecurity Executive Order So Far," *WIRED* (website), September 3, 2017, <https://www.wired.com/story/trump-cybersecurity-executive-order/>.

32. Chalfant, "Senators Demand."

33. White House, National Cyber Strategy of the United States of America, September 2018. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

National Guard personnel use of DoD information networks, software and hardware for State cyberspace activities.”³⁴

The second memorandum of note, Directive-Type Memorandum 17-007, coins the new term, “Defense Support to Cyber Incident Response” and clarifies the mechanism under DSCA to provide DoD cyber resources at the request of other federal agencies or SLTT governments through the DoD executive secretary. The memorandum clearly establishes a legal mechanism whereby DoD assets can be used for incident response and identifies situations in which support is not authorized, such as offensive cyberspace operations, defensive cyberspace operations response actions, or activities incident to military training.³⁵ These exclusions are consistent with the intent of the Posse Comitatus Act and in line with existing DSCA procedures.

As national policies on cyber defense and warfare have evolved, the Government Accountability Office has released several reports on the topic—specifically, DoD preparedness in responding to attacks on critical infrastructures. Three reports, summarized below, indicate disconnects in cyber incident planning continue to be addressed slowly.

The April 2016 Government Accountability report, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, clearly outlines three significant shortcomings in existing DSCA guidance. The report criticizes the absence of clearly defined DSCA roles and responsibilities in the event of a cyberattack. Second, it criticizes the Department of Defense’s lack of clarity on the defense organizations that would take the lead during a crisis.³⁶ The report highlights, for example, “US Northern Command’s DSCA response concept plan states that US 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 another command, US Cyber Command, would be responsible for supporting civil authorities in a cyber incident.”³⁷

A third criticism points out ambiguity in the roles and responsibilities of a dual-status commander—“the commander who has authority over federal military and National Guard forces” in the event of a cyber crisis.³⁸ In its response, the Department of Defense acknowledged the gaps in the roles and responsibilities and indicated it was continuing to develop its policies for DSCA response to cyber incidents.

34. John Tuohy, “Brigadier General John Tuohy’s Speech: National Guard’s Role in Cybersecurity for the U.S. Power Grid,” Lexington Institute (website), June 23, 2016, <https://www.lexingtoninstitute.org/brigadier-general-john-tuohys-speech-national-guards-role-cybersecurity-u-s-power-grid/>.

35. Robert O. Work, *Interim Policy and Guidance for Defense Support to Cyber Incident Response*, Directive Type Memorandum 17-007 (Washington, DC: Office of the Secretary of Defense, June 21, 2017).

36. Joseph W. Kirschbaum, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, DC: Government Accountability Office, April 2016).

37. Kirschbaum, *Civil Support*.

38. Kirschbaum, *Civil Support*.

The Department of Defense did not give a timeline for when it would finalize the policy.³⁹ Updated DoD Directive 3025.18 was published on March 19, 2018.

A second report, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises*, found National Guard units have developed various cyber incident response capabilities, but the Department of Defense may not be aware of these capabilities because they are not listed in a single database for quick recall in a time of crisis.⁴⁰ The Government Accountability Office asserts by not having this data, "DOD may not have timely access to these capabilities when requested by civil authorities during a cyber incident."⁴¹ The report also recommended the Department of Defense conduct a tier-1 exercise (involving "national-level organizations, combatant commanders and staffs in highly complex environments") to practice DSCA in response to a cyber incident. In its response, US Cyber Command indicated it is planning such an exercise.⁴²

A third Government Accountability Office report from November 2017, *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements*, rehighlights the Department of Defense's deficiency and inconsistency in DSCA policy for cyber incident response. The report identifies two additional recommendations. First, it advises the Department of Defense to update applicable cyber incident coordination training to be consistent with PPD-41; and, second, it recommends the Department of Defense maintain a list of senior departmental officials trained in the National Incident Management System to ensure it has a cadre of officials ready to go in a crisis response.⁴³

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM

The Protected Critical Infrastructure Information Program also impacts the Department of Defense. The Critical Infrastructure Information Act of 2002 established the program, which is managed by the Department of Homeland Security, to protect private-sector information related to critical infrastructure vulnerabilities with national security implications. The program sought to establish an information-sharing mechanism whereby nongovernmental entities could voluntarily exchange data with government organizations. This data exchange would be protected from Freedom of Information Act disclosure, state and local disclosure laws, and use in civil litigation.⁴⁴

The Protected Critical Infrastructure Information Program also established training and storage systems to protect the data that would only be accessible to

39. Kirschbaum, *Civil Support*.

40. Joseph W. Kirschbaum, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises*, GAO-16-574 (Washington, DC: GAO, September 2016).

41. Kirschbaum, *DOD Needs to Identify*.

42. Kirschbaum, *DOD Needs to Identify*.

43. Joseph W. Kirschbaum, *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements*, GAO-18-47 (Washington, DC: GAO, November 2017).

44. Critical Infrastructure Information Act of 2002, 6 U.S.C. § 671-4 (2002).

trained, authorized users with a need to know.⁴⁵ This information was to be used solely for national security and defense purposes. According to the under secretary of defense for policy website, the program allows the private sector to “more freely share sensitive and proprietary critical infrastructure information with government partners with the confidence that it will be protected from public release.”⁴⁶ In exchange, the government has access to information it otherwise would not. The government uses the information to analyze and secure critical infrastructures and protected systems, identify vulnerabilities, develop risk assessments, and enhance recovery preparedness measures.⁴⁷

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The National Cybersecurity and Communications Integration Center would likely be the first government organization to receive indications of a large-scale attack on US critical infrastructures. The center analyzes SLTT and private-sector cyber threat notifications and Protected Critical Infrastructure Information Program submissions.⁴⁸ The Department of Homeland Security formed this integrated command center in 2009 and eventually consolidated the National Communications System, National Coordinating Center for Communications, the US Computer Emergency Readiness Team, and the Industrial Control Systems Cyber Emergency Response Team into one organization. The National Cybersecurity and Communications Integration Center was codified in the National Cybersecurity Protection Act in 2014, and, according to the 2017 *NCCIC Year in Review* report, has since evolved to serve “as the federal-civilian interface for sharing cyber threat indicators” and coordinating response activities across all associated entities.⁴⁹

With this information sharing comes the enormous responsibility of protecting data and sources. The National Cybersecurity and Communications Integration Center is careful to share information responsibly while observing Americans’ civil liberties. The center works to build trust and transparency to ensure effective communications between organizations. The center was directly involved in the Department of Homeland Security monitoring of the integrity of the US election infrastructure before and during the November 2016 general election.⁵⁰ In addition, the center works with multiple international agencies and partners to counter the

45. Critical Infrastructure Information Act.

46. “Protected Critical Infrastructure Information (PCII) Program,” Under Secretary of Defense for Policy (website), n.d., <https://policy.defense.gov/OUSSDP-Offices/ASD-for-Homeland-Defense-and-Global-Security/Defense-Critical-Infrastructure-ProgramProtected-Critical-Infrastructure-Program/>.

47. “Protected Critical Infrastructure Information.”

48. NCCIC, *NCCIC Year in Review*.

49. NCCIC, *NCCIC Year in Review*.

50. NCCIC, *NCCIC Year in Review*.

global threat posed by cyberattacks.⁵¹ The center announced in its 2017 *NCCIC Year in Review* report it had:

- “[s]hared more than 15,600 alerts, bulletins, and other information products”;
- “[s]hared more than 3,000 indicators of compromise”;
- “[r]eceived more than 727,000 reported cyber and communications threats”;
- “[c]onducted 71 risk and vulnerability assessments for government and private sector clients”; and
- “[p]rovided on-site incident response support to roughly 30 government and private sector customers.”⁵²

Most recently, the 2015 Cyber Information Sharing Act made this information sharing possible. This law permits federal government organizations to share cybersecurity threat data with private-sector companies. The law also established a program in which private industry could voluntarily provide threat information to the government and be protected from criminal or regulatory liability.⁵³ This law is controversial; critics protest the potential for privacy-sharing violations between companies and the federal government.⁵⁴ A recent media report based on an National Cybersecurity and Communications Integration Center site visit indicates the center actively balances information exchange and the protection of consumer privacy as much as possible. As the center develops its data aggregation techniques, its degree of success in protecting consumers’ privacy remains to be seen.⁵⁵

In 2010, the Department of Defense and Department of Homeland Security signed a memorandum of agreement. This memorandum enables the agencies to collaborate on cybersecurity monitoring in near-real time and allows for the exchange of personnel between the two agencies and the sharing of automated threat data between the National Cybersecurity and Communications Integration Center and the National Security Agency Cybersecurity Threat Operations Center. The memorandum represented the beginning of the cooperation needed to share situational awareness and overcome cultural hurdles between the agencies.⁵⁶ Likely, the Department of Defense, through this agency, will first receive notice

51. NCCIC, *NCCIC Year in Review*, 11–15.

52. NCCIC, *NCCIC Year in Review*, 19–20.

53. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

54. “The Following Companies Just Betrayed Billions of People,” You Betrayed Us (website), n.d., <https://www.youbetrayedus.org/>.

55. Ashley Carman, “A Look inside the Department of Homeland Security’s Cyberhub,” *Verge* (website), May 6, 2016, <https://www.theverge.com/2016/5/6/11601248/nccic-tour-photos-cyber-attack-hq-dhs>.

56. Calvin Biesecker, “DHS, DoD Agree to Align Civil, Military Cyber Protection,” *Defense Daily* (website), October 14, 2010.

of a significant attack on homeland critical infrastructures and leverage shared information to apply DoD resources when requested.

PRIVATE-SECTOR INFRASTRUCTURE POLICY AND REGULATION ISSUES

Several issues complicate the use of DoD resources, especially as they relate to national security attacks on SLTT or private-sector critical infrastructures. As discussed earlier, the use of DoD personnel within the homeland is restricted. In times of crisis, SLTT organizations can request federal assistance through the Department of Homeland Security, which can then request DoD resources. Alternatively, the president can direct federal response from the Department of Defense, and certain standing authorities allow it to intervene to prevent damage or loss of life in an emergency.⁵⁷

Relatively new guidance in federal law, presidential directives, and DoD directives extends DSCA capabilities in support of cyber crises—specifically, attacks on critical infrastructure. Several issues, however, complicate the implementation of this assistance. The first issue is uncertainty about what constitutes an attack in cyberspace. History has shown hostile activity in cyberspace is not necessarily perceived as an armed attack that could lead to war, and attribution of the source of the attack is problematic. One might look to the effect of the attack or the intent of the attacker. The former can be deterministic, but the latter is more difficult to discern and requires deeper forensic investigation. Presidential Policy Directive 41 (PPD-41) provides a useful severity guide from an effects-based perspective, defining graduated responses based on how harmful or deadly the attack becomes.⁵⁸

The second issue is how a private entity or SLTT organization should request assistance, or even if it would want to request assistance in the first place. As the national focus on cybersecurity continues to develop, these organizations have invested heavily in their own internal cybersecurity. Some sectors have become quite good at detecting and remediating cyber threats by themselves. Ultimately, a private entity's request for DoD assistance would likely depend on the given scenario. For these reasons, many private entities may avoid asking for assistance.⁵⁹

The third concern is whether the Department of Defense has the expertise to respond in a decisive way. Critical infrastructure cyber systems have unique characteristics and protocols of which cyber responders within the Department of Defense may simply not be aware. Further, system architecture is different for each organization, and effective response requires intimate knowledge of the specific implementation. Without a working knowledge of the specific systems and their

57. Lynn, *Defense Support of Civil Authorities*, 1, 3–7.

58. Cilluffo and Cardash, “Overview and Analysis.”

59. “Assistant Secretary of Defense for Homeland Defense and Global Security Frequently Asked Questions,” Office of the Under Secretary of Defense for Policy, n.d., <https://policy.defense.gov/OSDPOffices/ASD-for-Homeland-Defense-and-Global-Security/Homeland-Defense-Integration-and-DSCA/faqs/>.

interconnections, protocols, and operating systems, an effective response with short notice is impossible.⁶⁰

In 2017, the US Navy conducted a critical infrastructure tabletop war game to assess current US policies. The war game involved a robust sampling of participants from across the federal government, various SLTT organizations, and private-sector infrastructure specialists. This war game was one of the first to bring together such a wide variety of players to address cyberattacks on critical infrastructure specifically. The war-game planners recognized the high degree of interdependence between domestic military missions and operations and private and SLTT critical infrastructure, including power and water for military facilities and transportation infrastructure for deployment operations.⁶¹ This interdependency is a potential vulnerability an adversary could take advantage of to impede military operations in the homeland and prevent power projection abroad. The war game sought to determine how severe or widespread a cyberattack on critical infrastructure needed to be to impact operations. The war game broadly found attacks would need to be targeted strategically both in time and location to cause a detrimental impact to national security. Likewise, the war-game report suggests if an attack is not targeted in both time and location, it will likely not have a severe impact on national security.⁶²

In addition, the Navy war game found private infrastructure owner-operators were not keen on seeking DoD resources when responding to a cyberattack. Among several possible reasons, the primary one was infrastructure owners feel responsible for their own cybersecurity and would call upon traditional first responders in local and state government for assistance in triage, remediation, and reconstitution in a catastrophic situation. In line with the Department of Defense structure for private-sector or SLTT security, the first touchpoint with the Department of Defense would be through a request for assistance from the Department of Homeland Security. The aforementioned reticence could be chalked up to the artificial nature of the war game and a lack of familiarity with or precedence in DoD capabilities in this type of crisis. Regardless, exercise directors noted this reticence as a significant observation in the war-game report.⁶³

On the other hand, private-sector owners opined the DoD assistance was appropriate in both passive defense of the nation's IT and telecommunications infrastructure and active defensive or offensive actions necessary to prevent or stop an attack.⁶⁴ Regardless, the implications of this war game are the Department of Defense needs to focus more on

60. Raj Chaudhary and Jared Hamilton, *The Five Critical Attributes of Effective Cybersecurity Management* (New York: Crowe Global, July 2015), 6-7.

61. Jacquelyn Schneider, Benjamin Schechter, and Rachel Shafer, *Navy-Private Sector Critical Infrastructure War Game 2017 Game Report* (Newport, RI: US Navy War College, July 2017), 2.

62. Schneider, Schechter, and Shafer, *Game Report*.

63. Schneider, Schechter, and Shafer, *Game Report*, 25.

64. Schneider, Schechter, and Shafer, *Game Report*, 25.

preattack deterrence and stopping adversaries during an attack rather than defense or reconstitution activities.⁶⁵

RECOMMENDATIONS

Currently, federal cybersecurity policy does not permit direct federal intervention in response to a cyberattack on private-sector critical infrastructure. Perhaps the best model for a military response is the Army and Air National Guard capabilities several states have been developing. Many members of National Guard cyber units are also employed in private industry in their respective states and have expertise on dual-use critical infrastructures (with civilian and military uses).⁶⁶ This expertise, combined with the unique authorities afforded to the National Guard under Title 32 (state status) and Title 10 (federal status) of the US Code, make developing National Guard capability the most promising avenue for bridging the gap between DoD countercyber response and private industry's desire to be free from federal intervention.⁶⁷ This approach leverages citizen-soldiers who potentially have working, day-to-day knowledge of the impacted equipment and the authority to protect national security during a crisis. These National Guard forces would need to be familiar with the elements of infrastructure that are essential to national security within their respective states and would need to participate in response and recovery training and exercises to hone their skills.

For a deeper DoD response, Cyber Mission Force National Mission Teams could train and become certified on the most critical infrastructures through public-private partnerships (with the invitation of private-sector stakeholders and SLTT organizations). Though having personnel in the active force with expertise on every infrastructure element is not feasible, an analysis of unit availability and capability and the corresponding critical, domestic missions would suggest where high-demand, low-density assets should be allocated. To minimize response time, establishing these relationships and familiarizing National Mission Team responders with critical infrastructure systems and networks before an adversary conducts a cyberattack of significant consequence is essential.

A third recommendation, inspired by the Defense Science Board, is to establish a national cyber defense plan for the cyber defense of homeland critical infrastructures that assigns responsibilities to the relevant agencies and acknowledges the existing legal authorities.⁶⁸ A 2017 report by the Defense Science Board concluded, "a more proactive and systematic approach to US cyber deterrence is urgently needed."⁶⁹ Such a deterrent

65. Jacquelyn Schneider, "Cyber Attacks on Critical Infrastructure: Insights from War Gaming," War on the Rocks, July 26, 2017, <https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/>.

66. Schneider, Schechter, and Shafer, *Game Report*, 24–25.

67. Schneider, Schechter, and Shafer, *Game Report*, 24–25.

68. Defense Science Board, *Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017), 12.

69. Defense Science Board, *Task Force on Cyber Deterrence*, 3.

strategy needs to be publicly documented, establishing redlines and clear consequences for violating standards, and must be known and communicated in advance. As recently highlighted by Senator Angus King of the Senate Committee on Armed Services, “[A] secret deterrent is not a deterrent.”⁷⁰

Finally, once roles and responsibilities have been established and agreed upon within the federal government, the Department of Defense needs to conduct tier-1 exercises that include interagency partners and span from the Combatant Command level down to the tactical level to integrate activities, responses, and battle rhythms and develop procedures for addressing a crisis. The United States cannot afford to allow the response to a significant attack on national security via critical infrastructure to be a pickup game. During such a crisis, preparation and strong interagency working relationships are key to a rapid recovery and ensuring the ability to continue operations in a degraded environment.⁷¹ Arriving on day one of a crisis fully prepared with the familiarity, skills, and interagency relationships and procedures to respond effectively with competence is imperative. A strong national security to prevent and rapidly recover from the potentially devastating effects of a targeted attack on US critical infrastructure is also imperative.

CONCLUSION

In a worst-case scenario, an attacker who directs a devastating cyber barrage at critical infrastructure at a strategic time and location could create a national security crisis with a high probability of success. Effective planning and coordination among stakeholders are crucial to prepare the nation to counter the effects of a determined adversary and ensure, if attacked, infrastructures degrade gracefully and can be reconstituted rapidly. Achieving these goals will not be an easy task given the wide array of private and governmental organizations that are responsible for operating critical infrastructure.

Clearly, the current statutory and regulatory environment does not readily permit the Department of Defense to respond to a significant attack on critical infrastructure. The existing structure led by the Department of Homeland Security is a coalition of the willing, untested by an actual crisis. While the early stages of a response structure are in place, shortcomings remain. The response, recovery, and reconstitution actions of the Department of Defense following an event should be provided initially by the National Guard with support from specially trained, active-duty National Mission Teams. Ideally, these cyber teams would follow a unified script spelled out in a national cyber defense plan that would be continually updated and improved through recurring tier-1 exercises that build upon lessons learned to train the next generation of responders. Through these actions, the likelihood of a debilitating cyberattack on domestic critical infrastructure would be greatly diminished.

70. Chris Galford, “Sen. King Presses Need for National Cyber Defense Plan,” Homeland Preparedness News (website), October 24, 2017, <https://homelandprepnews.com/stories/24919-sen-king-presses-need-national-cyber-defense-plan/>.

71. Defense Science Board, *Task Force on Cyber Deterrence*, 13–15.

APPENDIX A-2

FRAMEWORK FOR A CRITICAL INFRASTRUCTURE CYBER RESILIENCE ASSESSMENT

According to a study published by the North American Electric Reliability Corporation, “On December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers.”¹ Analysis of the outages revealed coordinated cyberattacks had taken place against Kyivoblenergo and two other regional electricity distribution companies in the Ukraine within 30 minutes of each other. An estimated 225,000 customers were impacted.² The sophistication of the attack and its targeting of Ukrainian infrastructure implicated Russia as the likely culprit. The incident became just one of the latest in a series of increasingly sophisticated and malicious attacks against advanced technology and, in particular, the critical infrastructure upon which the modern world is growing ever more dependent.³ Power failures during the cold winter months can certainly be inconvenient; however, cyberattacks that cause simultaneous disruptions across multiple critical infrastructure sectors during an international crisis requiring the mobilization and deployment of the military constitute a much more dangerous scenario. This part of the appendix proposes three approaches nations should adopt to address this threat.

- In the near term, emphasis must be placed on evaluating critical infrastructure and key resources both in terms of vulnerabilities and reliability and in the context of resilience.
- Secondly, manufacturers, system integrators, and asset owners must undertake a comprehensive effort to incorporate resilience engineering into life-cycle development, rather than implementing a solution after the fact.
- Finally, the United States and its allies and partners must globally advocate for international standards supporting the broadest adoption of security and resilience best practices possible.

Today, the United States and most modern societies rely upon a collection of advanced technologies to provide vital services to support daily activities. The services most Americans take for granted, such as electricity, clean water, and transportation, are considered to be critical infrastructure. To establish a common vocabulary and frame of reference, this part of the appendix uses US government definitions for the terms “critical infrastructure,” “system,” “security,” and “cyber resilience.”

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, defines critical infrastructure as the “systems and

1. Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (Atlanta, GA: North American Electric Reliability Corporation, March 18, 2016).

2. Lee, Assante, and Conway, *Analysis of the Cyber Attack*, 2.

3. Ron Ross, Michael McEvilly, and Janet Carrier Oren, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology (NIST) Special Publication 800-160 (Gaithersburg, MD: NIST, March 2018).

assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”⁴ The National Institute of Standards and Technology (NIST) defines system as “a combination of interacting elements organized to achieve one or more stated purposes. The interacting elements that compose a system include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities.”⁵ The institute also provides definitions for security and cyber resilience as they relate to critical infrastructure. Security, in the context of this discussion, is defined “as the freedom from those conditions that can cause loss of assets with unacceptable consequences.”⁶

Cyber resilience is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources,” regardless of the source.⁷ “Cyber resiliency supports mission assurance in a contested environment for missions that depend on systems which include cyber resources.”⁸ Systems security engineering concerns the systems, security, and cyber resilience for countering threats to critical infrastructure. The institute defines systems security engineering as a “specialty discipline of systems engineering. It provides considerations for the security-oriented activities and tasks that produce security-oriented outcomes as part of every systems engineering process activity with focus given to the appropriate level of fidelity and rigor in analyses to achieve assurance and trustworthiness objectives.”⁹ These terms provide a foundation for the assessment of critical infrastructure vulnerabilities, security, and resilience.

The first recommendation is for the establishment of a critical infrastructure assessment program within the US Army Reserve. Assessments could be conducted over the course of several assembly weekends and would culminate in a debriefing to the supported element. Figure A-2-1 outlines this program, including current Defense Critical Infrastructure Program requirements.

4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 42 U.S.C. 5195c(e) § 1016(e) (2001).

5. Ross, McEvelley, and Oren, *Systems Security Engineering*.

6. Ross, McEvelley, and Oren, *Systems Security Engineering*.

7. Ross, McEvelley, and Oren, *Systems Security Engineering*.

8. Ross, McEvelley, and Oren, *Systems Security Engineering*.

9. Ross, McEvelley, and Oren, *Systems Security Engineering*.



Figure A-2-1. Proposed critical infrastructure assessment program

The proposed team structure would be built with a reachback capability as required (see figure A-2-2). This capability would allow for simultaneously scaling the program up as mission requirements expanded and centralizing key subject matter experts in a supporting role.

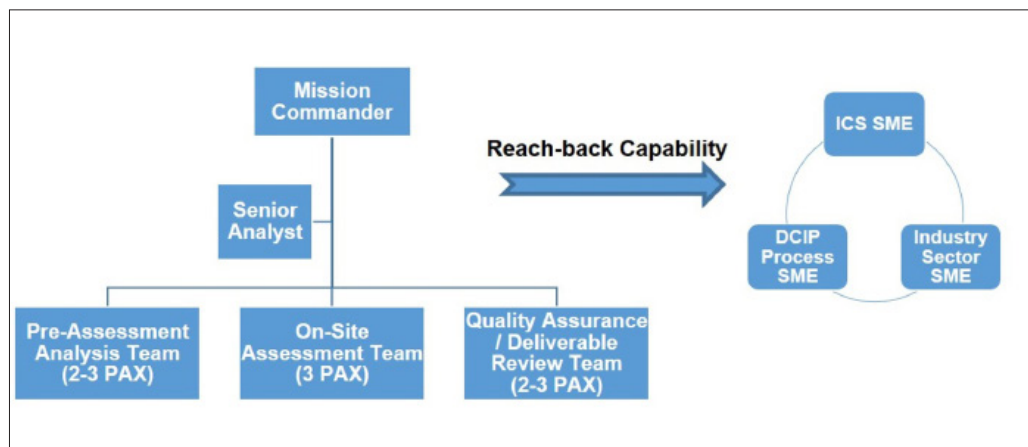


Figure A-2-2. Organization of proposed critical infrastructure assessment program

National security leaders need a way to assess these programs and understand their impact on the ability of the US military to mobilize and deploy its forces to respond to an international crisis. Several organizations have recognized the Department of Defense's (DoD's) dependence on public and privately owned critical infrastructure. The Defense Science Board Task Force on Resilient Military Systems and the Advanced Cyber

Threat warned, “[F]ull manifestation of the cyber threat could even produce existential consequences to the United States, particularly with respect to critical infrastructure.”¹⁰

One DoD response has been the creation of the Defense Critical Infrastructure Program. The program serves as the implementation of Chairman of the Joint Chiefs of Staff Instruction 3209.01. The Defense Critical Infrastructure Program is a “DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions.”¹¹ Under this program, the Department of Defense identifies Defense Critical Assets and Task Critical Assets.

Defense Critical Asset is “an asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of DoD to fulfill its mission.”¹²

A Task Critical Asset is “an asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or mission-essential task it supports.”¹³

The Defense Threat Reduction Agency created two programs to support this effort: the Joint Mission Assurance Assessment and Balanced Survivability Assessment.¹⁴ Though both of these assessments provide a comprehensive view of an asset’s vulnerabilities, the former assesses the impact of the vulnerabilities on the mission the asset is supporting.

The Department of Homeland Security also has several tools available for critical infrastructure asset owners to use in evaluating their environments. These tools include the Cyber Security Evaluation Tool and the Cyber Resilience Review (CRR).

According to the National Cybersecurity and Communications Integration Center, the Cyber Security Evaluation Tool is:

[A] desktop software tool that guides asset owners and operators through a step-by-step process to evaluate their industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations. . . . CSET helps asset owners assess their information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architectures, as well as operational policies and procedures. These questions are derived from accepted industry cybersecurity standards. When the questionnaires are completed, CSET provides a dashboard

10. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, December 2013), 23.

11. Pat Briley, “Defense Critical Infrastructure Program (DCIP),” *Guardian: The Source for Antiterrorism Information* 9, no. 2 (Fall 2007): 7.

12. Defense Contract Management Agency (DCMA), *Defense Industrial Base Critical Asset Identification and Prioritization*, DCMA Manual 3401-02 (Fort Lee, VA: DCMA, September 2018), 16.

13. DCMA, *Critical Asset Identification and Prioritization*.

14. Humphrey Barrera, “Cyber Resiliency and Survivability: The Defense Threat Reduction Agency’s (DTRA) Role in Cyber Assessments,” *Cyber*, July 1, 2016, <https://sites.google.com/a/milcyber.org/magazine/stories/resiliencyandsurvivability>.

of charts showing areas of strength and weakness, as well as a prioritized list of recommendations for increasing the site's cybersecurity posture.¹⁵

The CRR was developed in conjunction with the Carnegie Mellon University Software Engineering Institute's Computer Emergency Response Team Division as "a no-cost, voluntary, non-technical assessment" designed to help asset owners evaluate the operational resilience of an organization.¹⁶ The CRR is derived from the Computer Emergency Response Team Division's Resilience Management Model and has been tailored to organizations in the Critical Infrastructure Sectors identified by the Department of Homeland Security. The program allows for self-assessments or a facilitated option through the Department of Homeland Security. "The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices."¹⁷

While the focus of the CRR on the broader enterprise allows for a more holistic assessment, it does not address the configuration resiliency of industrial control systems directly. Understanding organizational resilience, vulnerabilities, and overall architecture shortcomings is essential; however, the emerging threat environment requires critical infrastructure stakeholders to consider shifting their focus toward cyber resilience. The dependence upon a wide variety of public and private sector industrial control systems by the Department of Defense and US society as a whole must be addressed as a key priority.

The second recommendation is the adoption of a framework for the comprehensive and consistent evaluation of the cyber resilience of critical infrastructure assets. This part of the appendix uses NIST Special Publication 600-180, Volume 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* as a foundation for assessing the techniques most likely to reduce the impact of adversary activity against a critical infrastructure asset. A driving assumption of this framework is an adversary is already operating within the networks and systems of the organization. The primary goal is to provide a mechanism for asset owners to assess the ability of their organization to remain functional despite adversary actions. The key techniques underlying the framework are adaptive response, coordinated protection, contextual awareness, diversity, dynamic positioning, nonpersistence, privilege restriction, realignment, redundancy, segmentation, substantiated integrity, and unpredictability.¹⁸

15. National Cybersecurity and Communications Integration Center (NCCIC), "NCCIC ICS Cyber Security Evaluation Tool," Cybersecurity & Infrastructure Security Agency, n.d., https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf.

16. "Assessments: Cyber Resilience Review (CRR)," Cybersecurity & Infrastructure Security Agency, n.d., <https://us-cert.cisa.gov/resources/assessments>.

17. "Assessments."

18. Ron Ross et al., *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160 (Gaithersburg, MD: NIST, November 2019).

Adaptive response is akin to an Army company commander applying his or her professional judgment to adjust force protection levels or increase security based upon an evolving threat environment within the area of operations. This technique leverages several approaches to provide critical infrastructure asset owners with a collection of courses of action to manage risks quickly and efficiently. Among these approaches, dynamic reconfiguration allows for changes to be made to “individual systems, system elements, components, or sets of cyber resources to change functionality or behavior without interrupting service.”¹⁹ Dynamic resource allocation allows for the reallocation of “resources to tasks or functions without terminating critical functions or processes.”²⁰ Adaptive management allows for alterations to how “mechanisms are used based on changes in the operational environment as well as changes in the threat environment.”²¹

Coordinated protection is a technique that ensures “protection mechanisms operate in a coordinated and effective manner,” similar to soldiers ensuring their force protection measures are included in a broader, regional force protection strategy (including supporting intelligence, surveillance, and reconnaissance; quick reaction forces; and fires) when operating from a forward operating base.²² Approaches that address coordinated protection include calibrated defense-in-depth, consistency analysis, orchestration, and self-challenge.²³

- Calibrated defense-in-depth is a proven approach within cybersecurity. The approach, which is recommended by the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, aligns well with initiatives currently underway at international standard organizations.²⁴ The goal of calibrated defense-in-depth is to provide overlapping controls at each layer of an architecture to dramatically increase the cost in time and effort required of an adversary.
- Consistency analysis and orchestration focus on the coordinated assessment of the various defense-in-depth control measures, ideally identifying complementary approaches and potential gaps within the overall infrastructure. Organizations must leverage their finite cybersecurity resources in the most efficient and effective manner possible.²⁵

19. Ross et al., *Developing Cyber Resilient Systems*.

20. Ross et al., *Developing Cyber Resilient Systems*.

21. Ross et al., *Developing Cyber Resilient Systems*.

22. Ross et al., *Developing Cyber Resilient Systems*.

23. Ross et al., *Developing Cyber Resilient Systems*.

24. Industrial Control Systems Cyber Emergency Response Team, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* (Washington, DC: Department of Homeland Security [DHS], September 2016).

25. Ross et al., *Developing Cyber Resilient Systems*.

- Self-challenge effectively tests and validates the control measures implemented as part of the overall coordinated protection effort to assess where improvements should be made or where coverage may be sufficient given the operating environment.²⁶

Diversity is a technique that uses “heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.”²⁷ This technique may be the most challenging to place into practice in large, commercial, critical infrastructure environments, but if it is applied across the board, it significantly raises the cost in time and effort required of an adversary to conduct an attack against large infrastructure. The steps taken at a technical level are similar to those espoused in the Army’s annual Level I Antiterrorism Awareness Training. A key tenet of the antiterrorism training for servicemembers traveling through areas where the risk of targeting may be increased is to avoid setting patterns or routines throughout the day. Similarly, diversity aims to confuse an adversary and make mapping a targeted network more challenging by incorporating unexpected technologies, control measures, design patterns, information sources, topologies, or suppliers.

Approaches involved in diversity include architectural diversity, design diversity, synthetic diversity, information diversity, path diversity, and supply chain diversity.²⁸

- Architectural diversity is the application of “multiple sets of technical standards, different technologies, and different architectural patterns.”²⁹
- Design diversity recommends using “different designs to meet the same requirements or provide equivalent functionality.”³⁰
- A good example of synthetic diversity would be implementation of “address space layout randomization.”³¹
- Information diversity includes the use of a variety of data sources.
- Path diversity allows for separate command, control, and communications methods to prevent an adversary from intercepting both application data and the command signaling. A good example of this approach is the use of “out-of-band channels.”³²
- The full scope of supply chain diversity extends beyond this discussion, but, as a best practice, organizations must carefully vet and monitor their key suppliers.

26. Ross et al., *Developing Cyber Resilient Systems*.

27. Ross et al., *Developing Cyber Resilient Systems*.

28. Ross et al., *Developing Cyber Resilient Systems*.

29. Ross et al., *Developing Cyber Resilient Systems*.

30. Ross et al., *Developing Cyber Resilient Systems*.

31. Ross et al., *Developing Cyber Resilient Systems*.

32. Ross et al., *Developing Cyber Resilient Systems*.

Dynamic positioning is a technique that focuses on the ability of an organization to reconfigure key systems and processes on demand. Approaches to dynamic positioning include functional relocation of sensors, functional relocation of cyber resources, asset mobility, fragmentation, and distributed functionality.

- Functional relocation of sensors is not unlike the steps taken by a company commander in conducting unexpected patrols in different areas. The goal is to disrupt adversary activity by being proactive and showing up in unanticipated locations.
- Functional relocation of cyber resources and, to an extent, distributed functionality are techniques in which specific processes are dynamically moved from one infrastructure to another.
- Cloud implementations offer enormous potential in this area by allowing organizations to shift resources as needed or in response to a perceived threat.
- Asset mobility is an extension of asset management, a best practice cited in several IT management system frameworks. Asset mobility is the ability of an organization to monitor the physical movement of a network-connected device from one part of the infrastructure to another.
- Fragmentation has long been used in redundant arrays of inexpensive disks to distribute the risk of hardware failure across multiple mathematically interlaced components. The failure of one component could be mitigated by the ability of the redundant arrays of inexpensive disks to reconstruct the data on the failed component through a collection of algorithms used to distribute slices of the data across multiple disks. Fragmentation can be considered in much the same way in this context.³³

Contextual awareness is a technique meant to allow for the creation and near-real-time updating of “current representations of the posture of missions or business functions considering threat events and courses of action.”³⁴ Approaches within this technique include dynamic resource awareness, dynamic threat awareness, and mission dependency and status visualization.

- The goal of dynamic resource awareness is to ensure consistent situational understanding. This approach calls for comprehensive insight into the overall environment, not just simple monitoring of the infrastructure and components.
- Dynamic threat awareness focuses on collecting, aggregating, and correlating relevant threat information into a concise and consumable format to support proactive mitigations.³⁵
- Mission dependency and status visualization is intended to support decision makers by providing an integrated view of the organization and its critical

33. Ross et al., *Developing Cyber Resilient Systems*.

34. Ross et al., *Developing Cyber Resilient Systems*.

35. Ross et al., *Developing Cyber Resilient Systems*.

processes.³⁶ One example of this is the emergence of cyber threat intelligence platforms, such as Hive-IQ from TeamWorx Security. Hive-IQ incorporates a variety of data sources and integrates them with artificial intelligence capabilities that help provide near-real-time collaboration and visibility into an environment.³⁷

Nonpersistence is a technique that focuses on only generating and retaining resources as needed. Approaches include nonpersistent information, nonpersistent services, and nonpersistent connectivity.³⁸ These ideas have been leveraged in military and commercial realms for decades. Soldiers have often been tasked with manning burn barrels to destroy sensitive papers that no longer needed to be retained. This requirement was often set by a command retention policy intended to prevent outdated yet sensitive information from being carelessly left unsecured in the back of a filing cabinet. Nonpersistent services and nonpersistent connectivity can be found within best practices for IT service management. Virtualized infrastructures allow for only using resources as required, rather than keeping separate physical servers for each service. Similarly, nonpersistent connectivity is used in the physical security realm where employee badges only allow access to buildings during normal business hours unless an exception has been specified.

Privilege restriction ensures a user, component, or service is only given access that is appropriate for the performance of the assigned tasks. Approaches within privilege restriction include trust-based privilege management, attribute-based usage restriction, and dynamic privileges.³⁹ These approaches are applied through the use of employee badges and access control measures. This technique ensures only the privileges required by a user, component, or service are extended, and they are extended in a controlled and auditable way. The principle of least privilege is a key aspect of privilege restriction because least privilege requires an adversary to overcome another hurdle (for example, gaining additional administrative rights) even if the adversary has already compromised the account in question. Dynamic privileges are a best practice when unique access is granted only under certain circumstances and is withdrawn when the circumstances no longer apply. Homeowners practice dynamic privileges when they call for a home repair. The repairman is granted access for the duration of the repair, his activities are monitored during this timeframe, and he is escorted to the door when the repairs have been completed. Repairmen are never granted unrestricted access again unless their services are required again.

Realignment is a technique that focuses on ensuring system resources are aligned “with current organizational mission or business function needs.”⁴⁰ Approaches within realignment include purposing, offloading, restriction, replacement, and specialization. Overall, these approaches are meant to simplify the operations of an

36. Ross et al., *Developing Cyber Resilient Systems*.

37. TeamWorx Security, “Hive-IQ Fact Sheet,” TeamWorx Security, n.d., <https://www.teamworxsecurity.com/wp-content/uploads/2021/06/Hive-IQ.pdf>.

38. Ross et al., *Developing Cyber Resilient Systems*.

39. Ross et al., *Developing Cyber Resilient Systems*.

40. Ross et al., *Developing Cyber Resilient Systems*.

infrastructure to reduce the size of the attack surface that is available to an adversary. The more unneeded systems and applications that can be decommissioned or removed from an environment, the less chance an adversary has to use them as a way into the target infrastructure. Purposing supports creating white lists and removing extraneous services. Specialization is a slightly different aspect of realignment because it recommends carefully engineered, custom components where they are critical to a mission or business function. The goal is to provide a highly controlled, trustworthy component that is tailored to the local environment.⁴¹

Redundancy is a technique that is designed to “provide multiple protected instances of critical resources.”⁴² Approaches within redundancy include protected backup and restore, surplus capacity, and replication.⁴³ Though certain critical infrastructure industries may require organizations to provide a certain percentage of redundant capacity, this technique implies a real cost for the asset owner. Investment in redundancy should be carefully weighed for its overall value in supporting critical mission and business functions. A good analogy is the allowance for bench stock within maintenance shops in the Army. A fully redundant capability would require every spare part for every vehicle serviced by the maintenance shop be maintained on-site to ensure the least downtime possible. Military leaders know this type of requirement is not practical or economically viable. Bench stock is based on multiple factors and optimized to keep the most mission-critical vehicles operational to the highest degree possible.⁴⁴ Similarly, in the critical infrastructure realm, asset owners should weigh their investment in surplus capacity and replication carefully and conduct realistic assessments on the likelihood the resources will be required and the frequency at which they will be required.

Segmentation is a technique that focuses on the separation of “system elements based on criticality and trustworthiness.”⁴⁵ This technique mirrors recommendations based on a survey conducted by the SANS Institute in 2017.⁴⁶ Establishing multiple control points allows for cybersecurity analysts to gain better visibility into an environment and makes an adversary’s maneuvers within a system or network after having gained access to it more difficult. Predefined segmentation and dynamic segmentation and isolation are approaches within this technique.

- Predefined segmentation is using the physical and logical design of applications, systems, components, and networks to separate different processes. One example is ensuring security tools and sensors are segmented from operational traffic. This measure prevents an adversary from gaining access to both an operational network

41. Ross et al., *Developing Cyber Resilient Systems*.

42. Ross et al., *Developing Cyber Resilient Systems*.

43. Ross et al., *Developing Cyber Resilient Systems*.

44. Martin D. Webb, “A New Approach to Class IX Control,” *Army Sustainment* 42, no. 4 (July–August 2010): 22.

45. Ross et al., *Developing Cyber Resilient Systems*.

46. Bengt Gregory-Brown, *Securing Industrial Control Systems – 2017* (North Bethesda, MD: SANS Institute, June, 2017).

and the security and sensor network and discovering everything the cybersecurity analysts know about the adversary's behavior.

- Dynamic segmentation and isolation, which is supported by new, software-defined networking capabilities, allows an organization to gain increasingly detailed control over its infrastructure.⁴⁷

Substantiated integrity is one of the core techniques of the framework recommended in this part of the appendix. Components that have incorporated this capability can “[a]scertain whether critical system elements have been corrupted.”⁴⁸ This technique is being vigorously pursued in the space system realm as the challenge of defending this environment grows more urgent. The parallels between substantiated integrity as proposed by NIST Special Publication 600-180 and runtime assurance in space-flight software are significant.⁴⁹ The approaches included in this technique are integrity checks, provenance tracking, and behavior validation.

- Integrity checks ensure the integrity of “information, components, or services.”⁵⁰ The goal of this approach is to ensure a process is performing as expected and within the parameters established by the operational environment.
- Provenance tracking is somewhat related to the supply chain diversity approach described above. The purpose of provenance tracking is to ensure any software, hardware, or related component incorporated into a component, system, or asset can be traced back to its origination and validated against attacks aimed at corrupting the supply chain itself.⁵¹
- Behavior validation considers the overall “patterns of prior usage” and establishes expected thresholds of performance.⁵² In the context of the operational environment, activities by a system outside of this threshold should raise an alarm that something unexpected has occurred.

Unpredictability is another technique related to the dynamic positioning and nonpersistence techniques described earlier. Approaches within unpredictability include temporal unpredictability and contextual unpredictability. The overall goal of these approaches is to keep an adversary off-balance and raise the cost in time and effort required to fully penetrate an environment.⁵³ This type of approach is often used in finance and accounting best practices to prevent a person from serving in a position of significant fiscal responsibility with no checks and balances. Many organizations

47. Ross et al., *Developing Cyber Resilient Systems*.

48. Ross et al., *Developing Cyber Resilient Systems*.

49. Wayne Wheeler et al., *Cyber Resilient Flight Software for Spacecraft*, American Institute of Aeronautics and Astronautics 2018-522 (Reston, VA: American Institute of Aeronautics and Astronautics, 2018), 15.

50. Ross et al., *Developing Cyber Resilient Systems*.

51. Ross et al., *Developing Cyber Resilient Systems*.

52. Ross et al., *Developing Cyber Resilient Systems*.

53. Ross et al., *Developing Cyber Resilient Systems*.

mandate employees in key positions (for example, comptroller) take a vacation for at least one or two weeks a year. During this timeframe, another employee steps in to assume the duties of the individual and can assess whether the individual is acting in the best interests of the organization and being a good steward of the organization's resources. Like a digital version of the checks and balances outlined above, the approach recommended by the National Institute of Standards and Technology would change system behavior in unpredictable ways to catch an adversarial process or attack that was counting on a static structure.

A key benefit of this framework is given its origins at the National Institute of Standards and Technology, one can expect to see integration of many of these techniques into the NIST Cybersecurity Framework for broader adoption across the operational technology and IT realms. The need to focus on the cyber resilience and integrated cybersecurity of individual components, systems, and assets, rather than performing simple assessments and applying mitigating control measures after the fact, continues to grow.

So far, the twenty-first century has presented significant challenges to the post-World War II world order. In a presentation at the 2017 International Conference on Cyber Conflict, then Chief of Staff of the Army Mark A. Milley argued, "[T]he character of war is evolving rapidly."⁵⁴ The *Summary of the 2018 National Defense Strategy of the United States* asserts the United States faces a security environment "defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest stretch of armed conflict in our Nation's history."⁵⁵

In "Kautilya's *Arthashastra* on War and Diplomacy in Ancient India," Roger Boesche discusses the statements of Indian statesman and strategist Chanakya (also known as "Kautilya" or "Vishnugupta") on war and diplomacy. Chanakya viewed conflict through the lens of competition. When considering other nation-states, one must identify which are "natural allies and which are inevitable enemies."⁵⁶ Chanakya's doctrine of silent war provides a relevant approach to analysis of the geopolitical situation today.⁵⁷ The silent-war concept in particular provides a lens through which one may assess Russia, China, and Iran's economic, informational, and offensive cyber operations "short of war" to extend their influence and dilute that of the United States and its allies.⁵⁸ These operations include "legal action, economic pressure, cyberattacks, and

54. Mark A. Milley, "The Future of Cyber Conflict" (speech, 2017 International Conference on Cyber Conflict, Washington, DC, November 7-8, 2017).

55. James Mattis, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: DoD, January 2018), 1.

56. Roger Boesche, "Kautilya's *Arthashastra* on War and Diplomacy in Ancient India," *Journal of Military History Online* 67, no. 1, (January 2003): 10.

57. Boesche, "Kautilya's *Arthashastra*," 10.

58. Ben Connable, Jason H. Campbell, and Dan Madden, *Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War* (Santa Monica, CA: RAND Corporation, 2016), 3.

terrorism,” and, in the case of China, appear to have been codified in a 1999 report by two senior Chinese military officers.⁵⁹

The concept of silent war aligns well with the operations these countries and other non-nation-state actors have been taking to further their interests around the world. “Silent war is a kind of warfare with another kingdom in which the king and his ministers – and unknowingly, the people – all act publicly as if they were at peace with the opposing kingdom, but all the while secret agents and spies are assassinating important leaders in the other kingdom, creating divisions among key ministers and classes, and spreading propaganda and disinformation.”⁶⁰ These operations are a key aspect of the changing character of war and the continuum of competition in today’s world.

China and Russia appear to be applying Chanakya’s concept of silent war in the realm of international standards and technical regulations. China has been a member of the World Trade Organization since 2001, and Russia, since 2012; as such, they are bound by the Agreement on Technical Barriers to Trade. This agreement “establishes rules and procedures regarding the development, adoption and application of standards, technical regulations and the conformity assessment procedures (such as testing or certification) used to determine whether a particular product meets such standards or regulations.”⁶¹

A recent report by the Office of the United States Trade Representative asserts, “China seems to be actively pursuing the development of unique requirements, despite the existence of well-established international standards, as a means for protecting domestic companies from competing foreign standards and technologies.”⁶² Aside from protection for its domestic industry, China appears to be using its World Trade Organization membership to gather foreign technology and intellectual property through one-sided licensing requirements while ignoring its obligations under the organization.

Russia also appears unwilling to apply transparent processes to their licensing requirements. According to the Office of the United States Trade Representative report, in the United States, electronics exporters “continue to raise concerns about the seemingly inconsistent application of the import licensing regime, absence of a written explanation when licenses are denied, issuance of licenses only for individual shipments rather than for all shipments of the ‘product family,’ requirement that information be submitted on a product-specific basis, rather than on a family-specific basis, and delays in issuing a license.”⁶³

The potential subversion of international standards is particularly noteworthy. The importance of international standards, technical regulations, and conformity assessments have only grown as societies pursue and adopt increasingly more advanced technologies in the twenty-first century. The United States and its allies and partners must continue

59. Connable, Campbell, and Madden, *Stretching and Exploiting*, 4.

60. Boesche, “Kautilya’s *Arthashastra*,” 22.

61. Robert Lighthizer, *2017 Report to Congress on China’s WTO Compliance* (Washington, DC: Office of the United States Trade Representative, January 2018), 58.

62. Lighthizer, *2017 Report*, 60.

63. Lighthizer, *2017 Report*, 14.

to support and advance the consistent development of international standards and best practices and encourage their transparent adoption globally.

This imperative applies to the realm of security as well. The mounting complexity of defense-related systems and their increasing reliance on commercial-off-the-shelf technologies require specific steps to be taken against the serious threat of an intentional or unintentional vulnerability finding its way into an operational system. These challenges include:

- “the increasing reliance on commercially available technology,”
- “complex supply chains that include thousands of suppliers worldwide,”
- “system interconnectedness,” and
- “the identification and exploitation of the supply chain and commercial off-the-shelf (COTS) vulnerabilities.”⁶⁴

Strategic leaders must have confidence in the trustworthiness of the systems employed. According to NIST Special Publication 800-53, trustworthiness “means worthy of being trusted to fulfill whatever requirements may be needed for a component, subsystem, system, network, application, mission, business function, enterprise, or other entity. Trustworthiness requirements can include attributes of reliability, dependability, performance, resilience, safety, security, privacy, and survivability under a range of potential adversity in the form of disruptions, hazards, threats, and privacy risks.”⁶⁵

The global continuum of competition and attempts by countries like Russia, China, Iran, and North Korea to gain advantage through silent-war tactics illustrate the risks that must be considered as US society becomes more dependent on technology from a wide variety of sources.

The development and publication of standards such as the International Organization for Standardization 27000 series on IT security and information security management systems were a giant leap forward in helping to pull together multiple fundamental principles and best practices in information security. Similarly, the International Electrotechnical Commission 62443 series of standards provides guidance for the industrial automation realm. The “series of standards, technical reports, and related information . . . define[s] procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.”⁶⁶

64. Paul R. Popick and Melinda Reed, “Requirements Challenges in Addressing Malicious Supply Chain Threats,” *INSIGHT* 16, no. 2 (July 2013).

65. Joint Task Force Interagency Working Group, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, 5th rev. (Gaithersburg, MD: NIST, September 2020).

66. “New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components,” International Society of Automation, September–October 2018, <https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c>.

The broad scope of International Electrotechnical Commission 62443 makes it particularly flexible as an international standard. The collection of technical requirements and guidance provides recommendations from the initial design and development of individual components to their integration into a system, their operation by an asset owner, and their decommissioning and secure disposal.

The comprehensive nature of the standard and its monitoring by multiple national and regional compliance agencies are helping to shift the discussion within the IT industry toward building in, rather than bolting on, security. Similarly, NIST Special Publication 600-180, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* encourages the use of systems security engineering practices that build on the international standards published by the International Organization for Standardization, the International Electrotechnical Commission, and the Institute of Electrical and Electronics Engineers. The special publication provides a clear and concise approach to incorporating security throughout the life cycle of a system, including the initial specification of requirements, acquisition, design, development, engineering, implementation, operation, and retirement.⁶⁷

According to the special publication, systems security engineering “helps to ensure that the appropriate security principles, concepts, methods, and practices are applied during the system life cycle.” Systems security engineering also “helps to reduce system defects that can lead to security vulnerability and as a result, reduces the susceptibility of the system to adversity.”⁶⁸ Systems security engineering provides an initial starting point toward improving the security of a system throughout its life cycle. But extending this approach and acknowledging the need for improving resilience, particularly within the critical infrastructure realm, are important. Considering the attack against the Ukrainian power distribution system, the security of the infrastructure itself becomes a secondary concern when weighed against the ability of the regional electricity distribution company to provide power to its customers. A new approach toward cyber resiliency is required. Volume 2 of NIST Special Publication 600-180 provides a framework for engineering practices that go beyond simple security and include the ability of a system to continue to function in the face of threats to it and its underlying components.

The application of international standards and best practices works well for new systems or those undergoing a significant technology refresh. Though future attacks will no doubt be unique in many aspects, conducting an ongoing assessment of techniques for ensuring the cyber resilience of critical infrastructure and key resources would provide additional insight into the ability of assets to continue operations while under attack or recovering from one.

The attacks against the Ukrainian power distribution system are only one example of the challenge facing critical infrastructure operators today. International standards, technical requirements, and processes for fair and transparent conformity assessment must be actively protected. The abuse of World Trade Organization membership by China and Russia and their disregard for their obligations and generally accepted

67. Ross, McEvilley, and Oren, *Systems Security Engineering*.

68. Ross, McEvilley, and Oren, *Systems Security Engineering*.

principles in these areas should be cause for alarm throughout the capitals of the developed world. The attempts by these countries to subvert and undermine many of the institutions that have evolved in the post-World War II era must be countered and challenged in the appropriate forums.

The United States and its allies and partners must continue to support the development and adoption of international standards, technical requirements, conformity assessments, and best practices designed to improve the security of twenty-first-century technology. Critical infrastructure assessments must evolve to include both traditional security controls and vulnerability assessments and an assessment of cyber resilience techniques. Though these cyber resilience techniques may not mitigate every potential attack, they help shift the discussion away from a strict focus on the prevention of an attack and toward continuity of operations during an attack.

The goal of the framework presented in this part of the appendix is to provide stakeholders with a more accurate picture of their environment and how it may continue to perform its mission. The reestablishment of a formal, ongoing, critical infrastructure assessment program is essential for providing national security leaders with a better understanding of the ability of critical infrastructure to continue to function during an attack. This reestablishment would provide a mechanism for evaluating the progress made toward improving the cyber resilience of assets over time.

APPENDIX A-3

COMMAND AND CONTROL OF DOMESTIC CYBER RESPONSE OPERATIONS IN A COMPLEX CATASTROPHE

In today's world, the nexus of the ever-accelerating depth and breadth of, and dependence on, cyber connectivity matched with the ever-growing capability and sophistication of malicious actors in the cyber domain creates significant vulnerabilities for societies and their governments. These vulnerabilities are most pronounced in the industries that provide essential services to the public and private sectors—especially cross-cutting services, such as electrical power, transportation, and water distribution. Large, successful attacks against these cross-cutting services would likely trigger compounding effects that could cascade across other services, causing widespread economic disruption and human suffering. To illustrate the severity of the problem, the US government experienced 77,000 successful cyberattacks in 2015—a 10 percent increase over the amount experienced in 2014.¹

Against the backdrop of this grim strategic landscape, this part of the appendix addresses the question of whether the Department of Homeland Security's (DHS) *National Cyber Incident Response Plan (NCIRP)* is sufficient to act as the command-and-control blueprint for a synchronized US response to a major, domestic, cyber incident, paying particular attention to DoD roles and responsibilities. Our methodology is the notional application of the tenets of the NCIRP to an unclassified and improbable, yet technologically possible, "significant cyber incident," as defined in the NCIRP, resulting in a complex catastrophic event.²

The NCIRP is the result of the trail of taskings, guidance, assessment, opinion, and policy that began with Congress, moved through the Government Accountability Office (GAO), and concluded with Presidential Policy Directive 41 (PPD-41). But would the NCIRP, in execution, fulfill the spirit of Congress's guidance, address GAO findings, and accomplish the intent of PPD-41?

The geopolitical aspects of the scenario used in this part of the appendix are the invention of the authors. The scenario is based on a Lloyd's and University of Cambridge Centre for Risk Studies study on the insurance impacts of a major cyberattack on the US electrical grid.³ The geopolitical factors of the scenario provide strategic context and desired complexity. The cyberattack portrayed in the Lloyd's and Centre for Risk Studies study presents a very challenging, large-scale scenario with catastrophic consequences. This study was deliberately selected to engage and stress the entirety of the provisions of the NCIRP and to maximize the extent of the likely federal defense support of civil authorities (DSCA) response.

1. Reuters, "US Hit by 77,000 Cyber Attacks in 2015—a 10 Percent Jump," *Newsweek*, March 21, 2016, <http://www.newsweek.com/government-cyber-attacks-increase-2015-439206>.

2. Department of Homeland Security (DHS), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016), 8.

3. Lloyd's and the University of Cambridge Centre for Risk Studies, *Business Blackout: The Implications of a Cyber Attack on the US Power Grid* (Cambridge, UK: University of Cambridge Centre for Risk Studies, May 2015).

BACKGROUND

In 2015, faced with mounting evidence of potential cyber vulnerabilities, Congress was understandably concerned about the ability of the United States to detect, respond to, and recover from attacks against military and civilian cyber infrastructure. The House of Representatives Committee on Armed Services report on the National Defense Authorization Act (NDAA) of 2016 explicitly noted the growing scope, sophistication, and destructive potential of such attacks and mentioned the possibility of DoD cyber capabilities being used in a DSCA role. “Although the Department of Defense generally does not resource support to civil authorities in response to a domestic cyber incident, the Department possesses an array of capabilities that may be requested when civilian response capabilities are overwhelmed or exhausted, or in instances where the Department offers unique capabilities not likely to be found elsewhere.”⁴

This language is a brief restatement of the key “request and provide” elements of the 1988 Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act) and is essentially the same phrasing used to describe the circumstances under which the DoD provides support to civil authorities in response to wildfires, floods, hurricanes, earthquakes, and other disasters.⁵

But the committee acknowledged the differences between the character and challenges of natural disasters and those of a potential major cyberattack. On these differing challenges, the report highlights “gaps in the Department of Defense’s plans and guidance for assisting civil authorities in the event of a domestic cyber incident.”⁶ Specifically, the report notes the DoD’s inability to accurately forecast the type or quantity of support that might be requested and the impediments to providing effective command and control for a likely admixture of military personnel under active duty (Title 10 of the US Code, federal command, and federally funded), full-time National Guard duty for operational homeland defense activities (Title 32 of the US Code, state command, and federally funded), and National Guard state active duty (SAD) (state command and funded by the state).⁷

The concerns of Congress were reflected in the NDAA, which directed the secretary of defense to “develop a comprehensive plan for the United States Cyber Command to support civil authorities in responding to cyber attacks by foreign powers . . . against the United States.”⁸ The NDAA also directed the DoD to conduct interagency-coordinated, biennial exercises that focus on responding to cyberattacks against critical infrastructure

4. Committee on Armed Services, National Defense Authorization Act for Fiscal Year 2016, H.R. Rep. No. 114-102 (2015), 289-90.

5. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707 (1988); and William J. Lynn III, *Defense Support of Civil Authorities, DoD Directive 3025.18* (Washington, DC: Under Secretary of Defense for Policy, updated March 19, 2018).

6. Committee on Armed Services, National Defense Authorization Act, 290.

7. Committee on Armed Services, National Defense Authorization Act, 290.

8. National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, 129 Stat. 1119 (2015).

“in consultation with Governors of the States and the owners and operators of critical infrastructure.”⁹

The NDAA required the DoD plan to include DoD internal training and exercises integrated and coordinated with other federal agencies; state and local plans and exercises; descriptions of the roles, responsibilities, and expectations of federal, state, and local authorities; and descriptions of the roles, responsibilities, and expectations of the active components and reserve components of the armed forces. Congress was sufficiently concerned about the challenges of a DSCA cyber response and the probability of such an occurrence that the NDAA, rather than simply requiring a DoD report on the matter, directed the GAO to review this plan.¹⁰

Over the course of 10 months and focused on the tasking contained in the Committee on Armed Services report to “assess the extent to which Department of Defense has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to cyber incidents,” GAO conducted a comprehensive survey of key US government, Department of Defense, and DoD components’ policies, guidance, strategies, and instructions on cyber operations and DSCA.¹¹ The survey consisted of a literature review augmented by interviews with senior leaders from the Department of Defense, Department of Homeland Security, United States Northern Command (USNORTHCOM), and the Federal Emergency Management Agency. In this assessment, GAO found, although the Department of Defense had developed and issued key DSCA guidance for the execution and oversight of DSCA, the guidance did not clearly define the roles and responsibilities of DoD components; the supported command (typically, USNORTHCOM); or any appointed, dual-status commander.¹²

The question of clarifying roles and responsibilities, as explored by the GAO report, points to a greater and more fundamental question: How exactly should the US government exercise whole-of-government command and control during cyber incidents? Several closely related documents subsequently published in 2016 sought to answer this question.

The first of these documents was PPD-41, *United States Cyber Incident Coordination*, published on July 26, 2016. The directive provided key definitions, announced principles to guide incident response, set lines of effort (LOEs), and assigned specific department and agency responsibilities.

Additionally, and most importantly for command and control, PPD-41 established lead federal agencies (LFAs) for specific LOEs during significant cyber incidents.

- Threat response LOE: LFA = Department of Justice (DOJ), through the FBI and the National Cyber Investigative Joint Task Force.

9. National Defense Authorization Act, 129 Stat. 1119.

10. National Defense Authorization Act, 129 Stat. 1119.

11. Joseph W. Kirschbaum, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, DC: Government Accountability Office, April 2016).

12. Kirschbaum, *Civil Support*.

- Asset response LOE: LFA = DHS, through the National Cybersecurity and Communications Integration Center (NCCIC).
- Intelligence support LOE: LFA = Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center.¹³

The directive also created two coordination entities: the standing policy coordination Cyber Response Group within the National Security Council and an on-call Cyber Unified Coordination Group (UCG). According to its charter, the UCG must coordinate among federal agencies and integrate “private sector partners into incident response efforts, as appropriate.”¹⁴ This interagency, collaborative approach is required because no single US government entity alone has the authority, capabilities, and expertise to effectively counter and resolve major cyber incidents.

The annex to PPD-41 provides additional details for the federal coordination architecture and directs the execution of certain implementation tasks. These tasks include numerous planning and coordination requirements for the sector-specific agencies responsible for the 16 Critical Infrastructure Sectors established by PPD-21, *Critical Infrastructure Security and Resilience*, in February 2013.¹⁵ The last paragraph of the PPD-41 annex directs the secretary of homeland security to achieve the following:

[I]n coordination with the Attorney General, the Secretary of Defense, and the SSAs . . . submit a national cyber incident response plan to address cybersecurity risks to critical infrastructure . . . that is consistent with the principles, policies, and coordination architecture set forth in this directive . . . [and] developed in consultation with SLTT governments, sector coordinating councils, information sharing and analysis organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals; [taking] into account how these stakeholders will coordinate with Federal agencies to mitigate, respond to, and recover from cyber incidents affecting critical infrastructure.¹⁶

In response to this tasking, DHS published the NCIRP in December 2016. Despite its title, the NCIRP is not a true plan. Rather, the NCIRP describes itself as a strategic framework document that “articulates the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure” and “establishes the strategic framework and doctrine for a whole-of-Nation approach to mitigating, responding to, and recovering from a cyber incident.”¹⁷

13. Barack Obama, *United States Cyber Incident Coordination*, Presidential Policy Directive 41 (Washington, DC: White House, July 26, 2016).

14. Obama, *Cyber Incident Coordination*.

15. Barack Obama, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (Washington, DC: White House, February 12, 2013).

16. Barack Obama, “Annex: Federal Government Coordination Architecture for Significant Cyber Incidents,” in Obama, *Cyber Incident Coordination*.

17. DHS, *Cyber Incident Response Plan*, 4, 6.

A COMPLEX CATASTROPHE

The scenario in this section could have come from today's headlines. A capable and well-resourced foreign power that has traditionally poor relations with the United States perceives a negative shift in American foreign policy. Next, strong US rhetoric further erodes the foreign power's relationship with the United States, which starts to label the foreign power as an adversary. Envisioning an increasingly confrontational future and knowing the decisive overmatch in conventional military capability, the foreign power begins to build a multidimensional, state-of-the-art, cyber warfare capability while initiating an intelligence campaign to identify exploitable cyber weaknesses in key US infrastructure. Over the next 18 months, as Washington's messaging becomes ever more hostile, foreign-power internal operatives and outsourced hackers of dubious morals analyze and defeat selected US power generation cybersecurity systems in the northeastern United States.¹⁸ Next, the operatives and hackers install custom-made malware in control rooms that directly manage power generator operations.

Once installed, the malware goes undetected and lies dormant. Covert efforts supported by the foreign power continue to infect ever-greater portions of the electrical generation capability. Ultimately, 100 sites are infected.¹⁹ Weak, erratic, soft-power attempts by the United States to influence foreign-power behavior and assemble a like-minded coalition are predictably unsuccessful, garnering the support of only a few, small, habitual allies in a tepid "coalition of the willing."

Finally, citing an allegedly egregious, amoral, regional action by the foreign power, a strident and politically isolated United States begins unilateral, in-theater, military deterrence measures and hints at "regime change" as a solution to the threat posed by the foreign power, now characterized as "bellicose and recalcitrant." The US government punctuates this equivocal, trial-balloon dialogue with highly publicized preparations for a significant, Joint, expeditionary, regional deployment.

The foreign power watches these developments with mounting dread and anxiety. With its diplomatic credibility in sharp decline, regime change in the wind, and the United States gearing up for regional combat, the foreign power decides to launch its cyberattack. The foreign power has no hope its cyberattack will derail US military preparations because the duration of the attack's effects may be limited, and the military has redundant systems and work-arounds that will likely minimize the impact of power outages on ongoing deployment activities. The cyberattack, however, might check the US administration's headlong rush into war if it is accompanied by the right information operations messaging.

On command, the malware releases its payload, which takes control of 50 vulnerable generators, forcing them into electrical overload.²⁰ The overload severely damages or destroys the generators and causes secondary explosions at a gas turbine facility. The resulting blackout impacts 15 states across Federal Emergency Management Agency Regions 1, 2, 3, and 5, which include Boston, New York City, Philadelphia, and

18. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout*.

19. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout*.

20. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout*.

Washington, DC.²¹ As the extent of the problem is realized, undamaged generators across the region are shut down as a precaution until the cause of the damage can be identified. Shutting down the generators amplifies the impact of the original attack and further inhibits efforts to restore power. The effects of this temporary but widespread destabilization of the regional electrical grid are catastrophic. Ninety-three million people are without electricity, mortality rates rise as health and public safety systems fail, and trade declines as port facilities and transportation systems collapse.²² In addition to these consequences envisioned by the Lloyd's and Centre for Risk Studies report, major urban centers would likely experience a spike in criminal activity and increased societal friction as the duration of the blackout grows.

On the heels of this attack, the foreign power sends a private, back-channel communication to the US president. This message admits responsibility for the attack and validates this claim by identifying the 50 generators that were damaged by the malware. This proof lends credibility to the foreign power's coercive threats, also contained in the message, of additional and more devastating attacks against other key US infrastructure systems. In exchange for staying its hand, the foreign power demands the United States slow its deployment and publicly eschew regime change.

Regardless of how the administration would respond to these events, the outlines of the national, domestic disaster response would be guided by the *National Response Framework (NRF)* and the NCIRP, and the military's DSCA contributions would be guided by DoD policy and regulation and Joint Publication 3-28, *Defense Support of Civil Authorities*. The time-tested, procedural path to employ federal military forces for domestic disaster response missions and to address the scenario's cyber and noncyber consequences begins at the local level.

As power is lost and essential services are impacted, local power companies and community first responders act to "save lives, protect property and the environment, meet basic human needs, stabilize the incident, restore basic services and community functionality, and establish a safe and secure environment moving toward the transition to recovery."²³ The magnitude of the attack and the geographic area impacted by the blackout is likely to overwhelm local resources quickly. As more counties turn to their state governors for assistance, and the state governments realize the extent of the disaster, the governors will declare a state of emergency, execute their state emergency action plans, mobilize portions of their National Guards under state active duty, and execute the appropriate emergency management assistance compacts.²⁴ If governors assess these measures will be insufficient to address the disaster, they may request federal assistance from the president, including, if necessary, a presidential declaration

21. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout*.

22. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout*.

23. DHS, *National Response Framework*, 2nd ed. (Washington, DC: DHS, May 2013), 1.

24. Stanley J. Czerwinski, *Emergency Management Assistance Compact: Enhancing EMAC's Collaborative and Administrative Capacity Should Improve National Disaster Response*, GAO-07-854 (Washington, DC: Government Accountability Office, June 2007).

of disaster or emergency under the Stafford Act.²⁵ If governors anticipate the use of federal military forces within their states, they may also proactively request the designation of dual-status commander.²⁶ One might reasonably guess some, but not all, governors would request and receive DSCA support.

Within this scenario, command and control for DSCA support, to supply emergency power and provide essential life support services and supplies to the various states, would largely resemble the structures employed for Hurricane Sandy in 2012. These structures fit the USNORTHCOM concept for structuring a “large-scale DoD response” (see figure A-3-1), with US Army North acting as the Joint Force land component commander and exercising command and control over several subordinate Joint task forces (JTFs), although the large-scale disaster in the scenario would likely call for adjustments to be made.²⁷ As a note, figure A-3-1 does not show the New Jersey JTF.

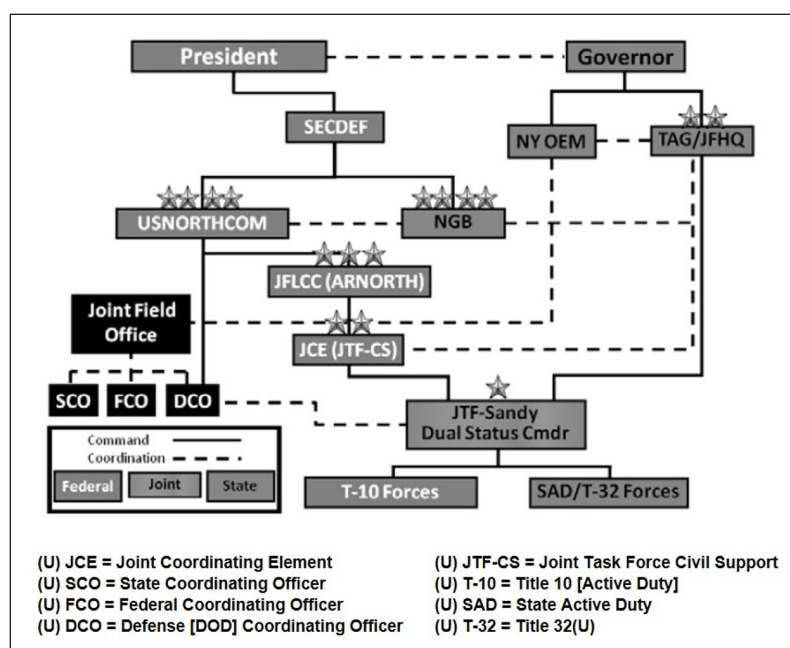


Figure A-3-1. Hurricane Sandy command and coordination

The scenario would call for multiple “JTF Sandy” organizations, one for each of the 15 states impacted by the power outage and requesting federal support. Only the states that employed subordinate, Title 10, active-duty forces would require a dual-status commander, who would exercise command authority simultaneously over Title 10,

25. Disaster Relief and Emergency Assistance Act.

26. Ryan Burke and Sue McNeil, *Toward a Unified Military Response: Hurricane Sandy and the Dual Status Commander* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, April 2015), 30.

27. Christopher D. Miller, *Defense Support of Civil Authorities*, CDRUSNORTHCOM CONPLAN 3501-08 (Peterson Air Force Base, CO: United States Northern Command, May 16, 2008), viii; and Burke and McNeil, *Unified Military Response*, 31.

Title 32, and SAD military units.²⁸ Dual-status commanders are the “usual and customary command and control arrangement in cases where Federal military and State National Guard forces are employed simultaneously in support of civil authorities within the United States.”²⁹

This dramatic expansion of state-level JTFs calls into question the ability of Joint Task Force Civil Support to exercise effective control, but USNORTHCOM has options to reinforce the standing structure of the Joint task force, if required. Likewise, the scenario may require multiple Joint field offices (JFOs), with one JFO serving as the primary office.³⁰ Fully staffing these multiple, interagency coordination nodes would be challenging for the affected states and agencies.

Turning to the cyber aspects of the scenario, other important differences emerge. Unlike damage caused by floods or tornadoes, damage caused by cyberattacks may be difficult to recognize at first. In the scenario, the information systems that were targeted, compromised, infected, and leveraged to damage US power generation are owned, operated, secured, and maintained by private-sector companies, either in-house or through contracted support. Because these companies are not part of the defense industrial base, they have no legal obligation to report information technology (IT) system anomalies, increased traffic (often an indicator of malware communicating with its controller), or IT security breaches.

Even if signs of an intrusion were detected, the information would likely not be voluntarily shared within the industry because of fears of exposing vulnerabilities, panicking investors, or damaging company reputations, credit, and industry standings. Moreover, even after the generator malfunctions have been correctly attributed to malicious intrusion and malware, private companies may hesitate to request government assistance. Such a request could ultimately demand a degree of system transparency and access that could compromise proprietary software and IT systems design or invite novice tinkering with systems and software that were previously opaque to outsiders. No private-sector IT systems manager wants a government body watching over his or her digital shoulder, nor does the manager want inexperienced “experts” attempting to fix a complex system they do not truly understand.³¹

Government assistance, however, may be a vital aspect of attack resolution. According to a report by the North American Electric Reliability Corporation, “[I]ndustry’s capability to analyze malware is limited and would require expertise likely

28. Daniel J. O’Donohue, *Defense Support of Civil Authorities*, Joint Publication 3-28 (Washington, DC: Joint Chiefs of Staff, October 29, 2018).

29. Leon E. Panetta, *Strategy for Homeland Defense and Defense Support of Civil Authorities* (Washington, DC: DoD, February 2013), 21.

30. O’Donohue, *Defense Support of Civil Authorities*, II-8.

31. Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes* (Washington, DC: Executive Office for United States Attorneys, 2015); and Dan Swinhoe, “Why Businesses Don’t Report Cybercrimes to Law Enforcement,” CSO, May 30, 2019, <https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html>.

available from software suppliers, control system vendors, or government resources.”³² Perhaps more importantly, “electricity system recovery and restoration would be delayed or may not begin until the nature of the cyber risks are understood [sic] and mitigation strategies are available.”³³ Collectively, these cyber-unique factors may combine to hinder preattack efforts to counter the malware threat; delay full postattack recognition of the threat; and impede investigative efforts to identify, eradicate, and protect against the threat. An additional element identified by researchers is the insufficient legal authorities necessary to overcome natural and institutional barriers to cooperation between government agencies and the private sector.³⁴

In the scenario, as in real life, private sector power-generating companies may neglect to approach a government entity for assistance. Conversely, every affected, private-sector, power-generating company may request government assistance. The middle ground—just some companies asking for help—is a reasonable assumption given the extent of the cyberattack and the severity of its consequences. But what help, specifically military help, would be available, and how might its command and control be best structured?

The National Guard has a robust and growing menu of cyber-capable organizations available for federal or state missions to support civil authorities in a cyber incident. The size, capabilities, and funding of these organizations vary widely among the 50 states, three territories, and the District of Columbia. The organizations’ capabilities generally fall into three categories: state communications directorates, which operate and maintain the state’s part of the National Guard information network (GuardNet); computer network defense teams tasked with protecting National Guard information systems against cyber threats; and National Guard cyber units, whose capabilities support the mission of USCYBERCOM.³⁵ Depending on the unit, these National Guard forces could conduct or support threat and vulnerability assessments, network analysis, penetration testing, remediation of cyber vulnerabilities, forensic operations, or cyber incident response and recovery efforts.³⁶

These National Guard capabilities could be available through SAD or Title 32 activation and assignment by state governors, although, as stated, private-sector companies may be reluctant to request help from military organizations. On the other hand, not knowing where or how the next cyberattack (if any) might fall, governors may be disinclined to assign their few, cyber-dedicated National Guard members to missions that would take them away from direct support of GuardNet and other state

32. North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report* (Atlanta, GA: North American Electric Reliability Corporation, March 2016), v.

33. North American Electric Reliability Corporation, *GridEx III Report*, 15.

34. Patricia Ladnier, “Critical Infrastructure Protection,” *InterAgency Journal: A Journal on National Security* 8, no. 3 (2017).

35. “Command, Control, Communications & Computers Directorate (J-6),” National Guard (website), n.d., <https://www.nationalguard.mil/Leadership/Joint-Staff/J-6/>.

36. Joseph W. Kirschbaum, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, DC: April 2016), 10–12.

cyber networks, particularly within this scenario, in which multiple power-generating sites in each state have been attacked and damaged. Additionally, isolating, defeating, and eradicating the malware from the networks of potentially several different companies and their many separate sites would severely strain the capacity of even the largest and most capable National Guard cyber units.

These challenges—particularly information sharing and full access—are likely to be further complicated by the hiring of independent cyber support contractors by private-sector companies, both before and after the cyberattack. Even companies that were not initially attacked may fear the presence of malware in their IT systems. This fear could create a cyber version of the “civilians on the battlefield” conundrum that has long confronted conventional forces. Working out the triangular relationship among company IT leaders, contracted support, and military assistance forces would be exceptionally challenging. In this scenario, deconflicting the battlespace by not assigning military assistance to the companies employing third-party contract support might be the best option.

At best, National Guard units in some states could be helpful if they have been requested by a private-sector company and granted the appropriate access. In addition, the units would need to be able to resolve any legal or privacy impediments favorably and to access Top Secret information while in SAD or Title 32 status (currently denied by DoD policy). Furthermore, the units would need to be available and not committed by the governor to a higher-priority task or contingency. The chances of these conditions being met are slim, but they are not impossible. Thus, in a DSCA response to an attack, one should assume limited National Guard personnel will be assigned to provide cyber support to companies. But what about federal support, especially military support?

The NCIRP and its parent guidance, PPD-41, would guide the organization and employment of federal support in a response to a cyberattack. The directive and the NCIRP specify LFAs for each of the three LOEs and identify the key tasks within the LOEs. This overarching federal structure is shown in figure A-3-2.

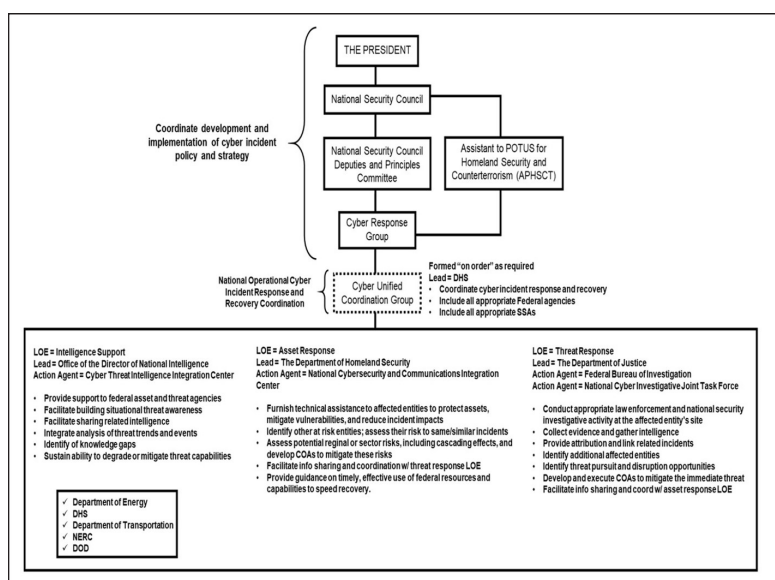


Figure A-3-2. NCIRP federal structure for cyber incident response

In the scenario, DHS leads the Unified Command Group, which includes the three LOE leads (per PPD-41 and the NCIRP) plus the Department of Energy, DHS, and the Department of Transportation as affected sector-specific agencies (again, per PPD-41 and the NCIRP).³⁷ The Department of Defense is included in the UCG because of the probability of support being provided by USCYBERCOM and because of the depth of DoD expertise in cyber operations and defense. The private, not-for-profit North American Electric Reliability Corporation is included in the UCG because of its expertise in ensuring the reliability of the bulk power system in North America. The National Security Agency is part of the Department of Defense and operates under the authority of the Office of the Director of National Intelligence. Because the National Security Agency is subsumed by the Office of the Director of National Intelligence as the lead federal agency for the intelligence support LOE, the agency is not called out in the diagram.

A fourth LOE is identified in the NCIRP—the “affected entity’s [internal] response activities”—but the NCIRP also states, “the Federal government typically will not play a role in this line of effort.”³⁸ These statements suggest, but do not prohibit, the use of federal (including DoD) cyber response capabilities—perhaps even in support of private enterprise. But a policy that indicates a potential for federal “rescue” may de-incentivize the development of robust cyber defense capabilities in the private sector.³⁹ Nevertheless, some literature suggests DoD capabilities are no better than those of private industry, albeit this reporting is at an unclassified level.⁴⁰ If the Department of Defense had nothing more to offer, then the discussion of DoD involvement in private-sector cyber incident response would be moot.

Despite these issues and concerns, the NCIRP does provide guidance for federal—and, thus, DoD—participation in cyber incident response. On the threat response LOE, the NCIRP states the “DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces.”⁴¹ This passage specifically identifies an LFA request as the initiation point of support, although the original request could originate with a civil authority. For the DoD, this terrain is comfortable. The department routinely supports other federal agencies under the authority of the Economy Act of 1932. A request from the Department of Homeland Security or the Department of Justice as the LOE lead would be sent to the Office of the Secretary of Defense through the Joint Staff for validation and sourcing along a path similar to a Combatant Commander’s request for forces.

37. Obama, *Cyber Incident Coordination*.

38. DHS, *Cyber Incident Response Plan*, 5.

39. Rob K. Knake, “Spotlight on Cyber VI: Respecting the Digital Rubicon: How the DoD Should Defend the US Homeland,” *Georgetown Journal of International Affairs* (website), December 7, 2016, <https://www.georgetownjournalofinternationalaffairs.org/online-edition/respecting-the-digital-rubicon-how-the-dod-should-defend-the-u-s-homeland>.

40. Penny Crosman, “Inside Wells Fargo’s Cybersecurity War Room,” *American Banker* (website), July 31, 2017, <https://www.americanbanker.com/news/how-wells-fargos-cyber-warriors-stay-battle-ready>.

41. DHS, *Cyber Incident Response Plan*, 14.

Given the scenario, any reasonable request that did not place higher-priority missions at risk would almost certainly be granted. But whether these DoD assets could be used in support of the private sector, rather than in the more limited and specific support of civil authorities, as is stated in the NCIRP is uncertain. Yet in the scenario, with no civil authority cyber networks under attack, determining the rationale officials would use to justify a request for DoD cyber support is difficult. Perhaps a governor, having used his or her own National Guard cyber capabilities to support a request from the private sector or to protect National Guard or other state networks, could request DoD support to augment their own limited resources. But such an action by a governor would cause active-duty DoD personnel to indirectly support the private sector, which is a legal issue, or to backfill National Guard personnel in state duties while they support private sector victims, which would be nonsensical. Similar concerns influence DoD forces acting within the asset response LOE.

On the asset response LOE, the NCIRP states, “Federal asset response support to the private sector from the NCCIC in the form of on-site technical assistance is generally contingent on a request from or consent of the supported entity.”⁴² This language specifically identifies the private sector as the recipient of “Federal asset response,” but, unlike the threat response paragraph, the language does not mention the DoD. The language also implies a request is originating from the private sector and going to the NCCIC, perhaps directly or perhaps through the DHS as the LFA for the LOE or the lead for the UCG. Once again, this situation is not representative of a traditional DSCA request process because the commercial entity would be supported, not a civil authority.

Whether DoD assets would be allowed to fulfill a support request from a private entity through the NCCIC is uncertain. To do so, the NCCIC would need to already have, or request through DHS under the Economy Act, DoD support that could be passed down to the commercial entity. But despite no legal hindrances preventing the DoD from supporting another federal agency, significant legal and privacy impediments prevent the DoD from becoming directly involved with private enterprise.

Additionally, the command of individuals, teams, and units provided to other agencies is never outside the normal DoD chain of command, and Combatant Command authority for cyber personnel would remain with USCYBERCOM. In practice, this support to other federal agencies would be akin to temporary duty for individual augmentees or direct support for teams and units, with the direct support (or other) relationship being assigned by the Combatant Commander.⁴³ Units provided in a direct support relationship may not be subdivided or reassigned by the supported unit. In this context, for DHS or the NCCIC to abide by “the letter of the law” in a direct support relationship and still use DoD assets in support of a private entity would be extremely difficult, even if such use were permissible under federal law.

If DoD resources were able to support either of these LOEs, the support would almost certainly be resourced from USCYBERCOM, where virtually all of the DoD’s cyber expertise resides. United States Cyber Command’s three main focus areas are

42. DHS, *Cyber Incident Response Plan*, 18.

43. Headquarters, Department of the Army (HQDA), *Operational Terms*, Field Manual 1-02.1 (Washington, DC: HQDA, March 2021), 1-32.

“[d]efending the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation’s ability to withstand and respond to cyber attack.”⁴⁴ The command organizes its 5,000 cyber personnel around these main focus areas with three types of functional teams: National Mission Teams (NMTs) (13 teams) to “defend the United States and its interests against cyberattacks of significant consequence”; Cyber Protection Teams (68 teams) to “defend priority DoD networks and systems against priority threats”; and Combat Mission Teams (27 teams) to “support Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations.”⁴⁵ Twenty-five additional teams provide planning and analytical support to the Combat Mission Teams and NMTs.⁴⁶ As of October 2016, all 133 of these teams had achieved initial operational capability and were on path to reach full operational capability in 2018.⁴⁷ Figure A-3-3 maps the most likely relationships among USCYBERCOM main focus areas, USCYBERCOM teams, and NCIRP LOEs.

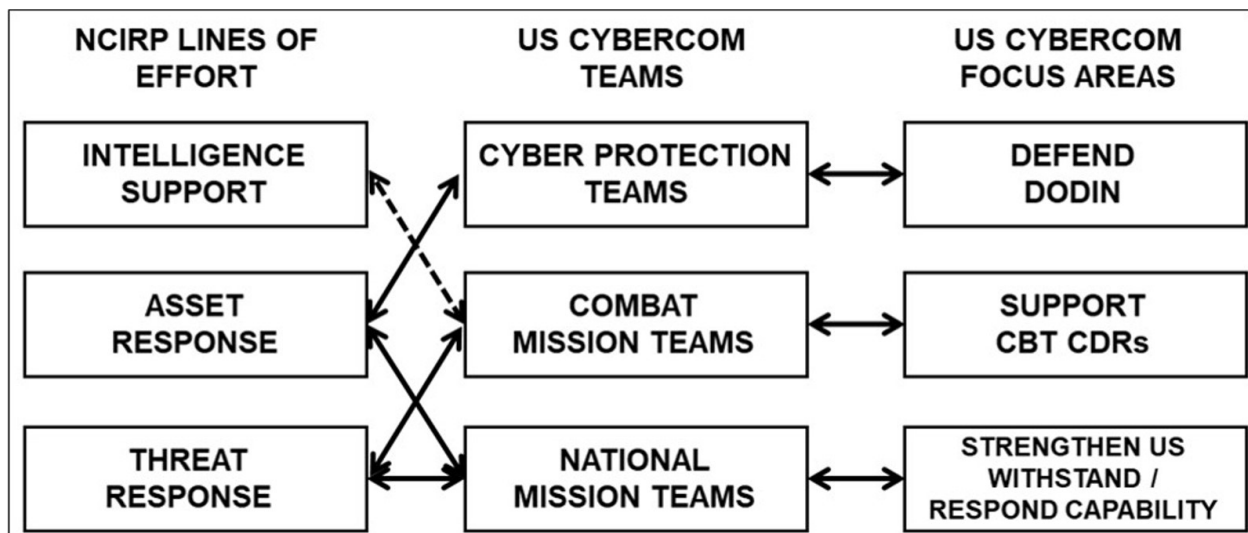


Figure A-3-3. Line of effort (LOE) and USCYBERCOM crosswalk

The putative relationships between USCYBERCOM teams and NCIRP LOEs contain some anomalies and inherent challenges. First, although the intelligence support LOE and USCYBERCOM teams do not seem to be connected, the NCIRP states, “The

44. “Our Mission and Vision,” United States Cyber Command (USCYBERCOM) (website), n.d., <https://www.cybercom.mil/About/Mission-and-Vision/>.

45. DoD, *The Department of Defense Cyber Strategy* (Washington, DC: DoD, April 2015); and “Our History,” USCYBERCOM (website), n.d., <https://www.cybercom.mil/About/History/>.

46. C. Todd Lopez, “Commander Discusses a Decade of DOD Cyber Power,” DoD (website), May 21, 2020, <https://www.defense.gov/Explore/News/Article/Article/2193130/commander-discusses-a-decade-of-dod-cyber-power/>.

47. USCYBERCOM, “All Cyber Mission Force Teams Achieve Initial Operating Capability,” DoD (website), October 24, 2016, <https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/>.

DoD actively characterizes and assesses foreign cybersecurity threats and informs the relevant interagency partners of current and potential malicious cyberactivity. Upon request, the DoD intelligence components may provide technical assistance to US government departments and agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy.”⁴⁸

Interestingly, this language is virtually identical to the roles and missions ascribed to the National Security Agency’s Cybersecurity Threat Operations Center.⁴⁹ Thus, the role USCYBERCOM might fill is unclear, and a support request from the Office of the Director of National Intelligence is highly unlikely – particularly because, presently, the National Security Agency and USCYBERCOM are so closely tied together.

Secondly, having enough troops available for cyber support would be problematic. Based on NCIRP language and USCYBERCOM mission capabilities, if a sourcing request were submitted, it would probably be for threat response and probably come from the FBI or the Department of Justice. Both the Combat Mission Teams and the NMTs seem suited for threat response tasks. But how many, if any, of the 27 Combat Mission Teams dedicated to the nine Combatant Commands would be available for the tasking is unclear, particularly because of the regional deployment and combat operations implied by the scenario. This problem might force the 13 NMTs to perform their routine USCYBERCOM missions while also covering any requests emanating from the threat response LOE and, perhaps with Cyber Protection Teams, the asset response LOE.

To exacerbate this problem and diminish the pool of DoD resources available to address the cyberattack, the foreign power may opt to conduct a series of supporting cyberattacks against the DoD Information Network or other infrastructure targets. These attacks need not be sophisticated or even successful; they would only need to be high-volume and persistent to consume DoD resources. A lesser alternative that might achieve the same effect would be to create a cyber deception with a dramatic spike in terrorist or jihadi Web chatter involving attack plans against US civilians to divert analytical capability and dilute federal efforts against the real cyberattack. Given the scenario and these possible additional stressors, the cyber capability demand would perhaps be greater than the cyber warrior supply, and the DoD would have to make some difficult prioritization decisions.

FINDINGS

This part of the appendix began by posing the question of how the US government should exercise whole-of-government command and control during cyber incidents. Next, strategic documents were explored to understand the current guidance and policies that would influence command-and-control decisions. The documents were scrutinized through the lens of a challenging, multifaceted cyberattack scenario and tempered by professional judgment to further refine the thinking on cyber command and control at the implementation level. By overlaying the template of the NCIRP with

48. DHS, *Cyber Incident Response Plan*, 20.

49. DHS, *Cyber Incident Response Plan*, 20.

the scenario-based realities of execution, including a simultaneous, conventional DSCA effort, a picture emerges that suggests a reasonable construct for whole-of-government command and control of large-scale cyber response efforts. This tentative concept is shown in figure A-3-4.

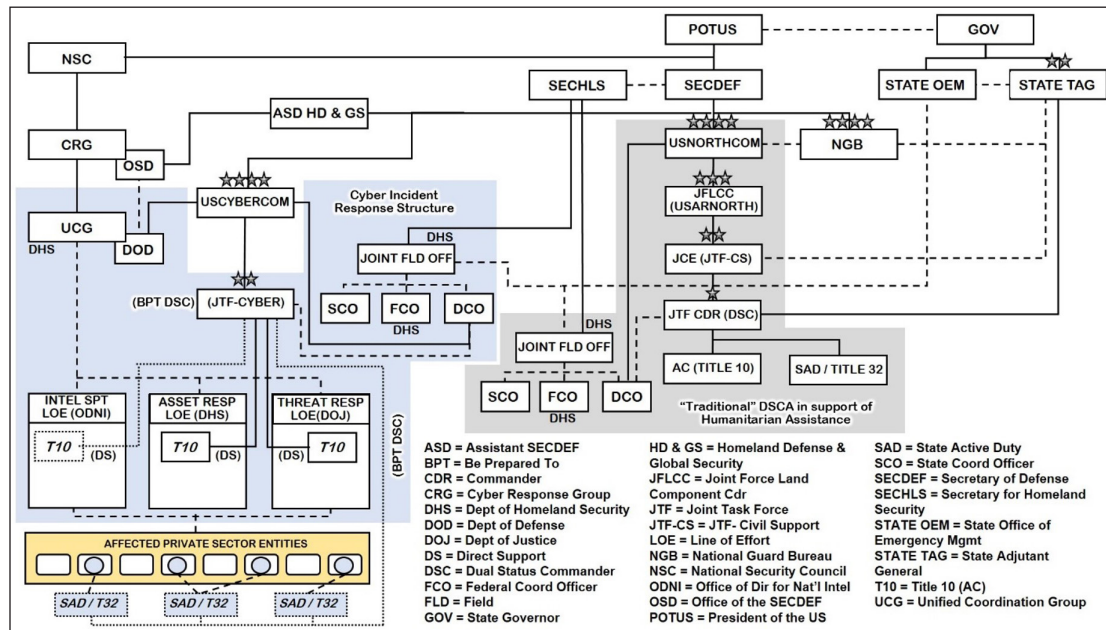


Figure A-3-4. Tentative structure and command and control

GENERAL

Figure A-3-4 depicts the simultaneous employment within a single state of traditional humanitarian assistance DSCA (in gray area) and the cyber incident response structure (in blue area). The affected power-generation private-sector entities, which would be more numerous than illustrated here, are backlighted in gold. The humanitarian assistance DSCA and the cyber incident response structure are stand-alone in that one does not require the existence of the other to be fully functional. Solid lines represent command relationships. Dashed lines represent support or coordinating relationships. Dotted lines represent possible future command relationships and are explained more fully later. The humanitarian assistance DSCA structure and command relationships are adapted from figure A-3-1 and not explained further here.

NATIONAL SECURITY COUNCIL/CYBER RESPONSE GROUP/UCG

These organizations and their relationships were explained earlier. A complete discussion of these organizations can be found in PPD-41 (and its annex) and the NCIRP. In the Cyber Response Group, the DoD representation is provided by the Office of the Secretary of Defense through the assistant secretary of defense for homeland defense

and global security, which offers the best alignment of responsibilities.⁵⁰ United States Cyber Command provides the UCG's DoD representative.

JOINT FIELD OFFICE (JFO)

Likely, many JFOs would be created to support a complex disaster of the scale presented in the scenario, but, for clarity's sake, only a single JFO is shown here. The internal structure of the JFOs for cyber incident response would be similar to that of the JFO for humanitarian assistance DSCA. The Information Technology – Information Sharing and Analysis Center, however, is included in the cyber response JFO structure to facilitate information sharing through the center's structure and processes. The defense coordinating officer is sourced from USCYBERCOM, rather than USNORTHCOM, to provide the necessary cyber expertise and to leverage his or her deep knowledge of USCYBERCOM's organization and capabilities.

JOINT TASK FORCE (JTF) CYBER

Cyber response operations and the employment of military personnel, teams, and units will vary from state to state and will be distributed over a large geographic area. Provided the span of control is not overwhelmed and effective communications can be established and sustained, a single JTF could provide command and control over the entire DoD cyber response effort. If these conditions are not met, multiple JTFs would have to be created. The limiting factor in creating multiple JTFs would be communications capability and the capacity and depth of qualified personnel resources. These limiting factors would apply in particular to JTF commanders and key staff, who would need an in-depth understanding of the cyber domain, cyber operations, and USCYBERCOM. Absent this understanding, JTF commanders may be unable to exercise effective mission command over cyber response forces.

Based on the guidance implied by the language in the NCIRP and accepting the high probability of legal restrictions on the use of active component forces in working directly with private-sector entities, the structure presented here separates active component and National Guard capabilities. Most likely, the Department of Homeland Security and the Department of Justice, acting as LOE leads, would request DoD support. This request is shown by the solid lines surrounding the T10 boxes within the LOE portion of the diagram. The relationship between the DoD capabilities and the federal requesting agency is equivalent to direct support, which is shown with the annotation "(DS)" on the diagram. Department of Defense support to the intelligence support LOE is possible, but unlikely, as indicated by the dotted lines.

Joint Task Force Cyber would exercise operational control over the assigned active component forces.⁵¹ Because of the likely preponderance of active component cyber support forces being employed, JTF commanders would have to be active

50. "Defense Critical Infrastructure Program Roles & Responsibilities," Under Secretary of Defense for Policy(website), n.d., <https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Global-Security/Defense-Critical-Infrastructure-Program/Roles/>.

51. HQDA, *Operational Terms*, 1-74.

component officers. Moreover, because of the specialized knowledge required, these officers would most likely be sourced by USCYBERCOM.

Joint Task Force Cyber (or multiple JTFs) could be sourced by USCYBERCOM component commands. The command is already moving in this direction with the establishment of Joint Force commands within each of its components. These commands are tasked with supporting designated, geographic Combatant Commands with cyber support.⁵² These standing headquarters arrangements allow USCYBERCOM to structure, man, and equip the organizations to suit the unique needs of the cyber domain and to tailor them to specific missions as required. This arrangement will also enable the development of standing procedures for alert, deployment, operations, and recovery. Routinely using these headquarters in national exercises would support the development of lessons learned that would inform future JTF operations and procedures and the greater US military cyber domain community.

State active duty (SAD)/Title 32 National Guard forces serve in either status. This proposed structure assumes National Guard organizations within the states have sufficient depth of expertise and the legal authority to offer cyber support to affected private-sector entities within their states and private-sector entities will request and accept assistance. These efforts may be episodic and will not include all affected entities. National Guard forces performing these missions would not be “federalized” for domestic cyber response because the situation within the scenario does not meet the criteria of foreign invasion, insurrection, or lawlessness required by federal law.⁵³ Because these National Guard forces could be conducting missions parallel to the federal effort within the LOEs, they should fall under a common commander for the purposes of unity of effort and synchronization. For this reason, each JTF Cyber commander must be prequalified as a dual-status commander and must be prepared to exercise operational control over all military forces supporting the cyber response in the event SAD or Title 32 forces begin supporting the effort—as annotated by “(BPT DSC)” in the diagram.

CONCLUSION

As this part of the appendix has shown, the impediments to rapid and effective cyber response operations to address a complex catastrophe are numerous and highly nuanced. Law, policy, paucity of expertise, private-sector resistance, immature coordination structures, an uneven distribution of capabilities and authorities, and lack of large-scale, high-level exercises combine to create significant institutional friction. Although limited in scale, previous exercises like GridEx and Cyber Guard have made significant contributions to the collaborative examination of problems and exploration of solutions in a field largely unfettered by precedent. This part of the appendix may serve as a foundation for an alternative methodology for approaching the question of cyber response command and control. It presents a workable structure and its associated command and support relationships based on policy, strategy, and existing regulatory

52. USCYBERCOM, “Cyber Mission Force Teams.”

53. Chief and Assistant Chief of Staff of National Guard Divisions and Wings in Federal Service: Detail, 10 U.S.C. § 12502 (1994).

guidance and provides a possible new end state for future exploratory efforts. Knowing the end allows one to marshal deliberately the ways and means in a manner that decisively contributes to achieving the end state.

Over the last decade, the United States has shown itself to be prepared to meet the challenges of fire, flood, and storm effectively and efficiently at a national level. The nation must now dedicate itself to preparing to meet the cyber storm. Effective organization and clear command and control will be critical to this preparation and execution. If the future looks like the recent past, the nation has no time to lose.

APPENDIX B

IMPACTS OF FULL MOBILIZATION IN THE CONTESTED HOMELAND

The US Army depends on the reserve component to deploy during full mobilization. In a contested homeland, however, the reserve component may have to compete with other government agencies and critical industries for priority as it mobilizes. During full mobilization, significant issues for both reserve soldiers and their civilian employers will be encountered as the soldiers extricate themselves from work and report for duty with the US Army Reserve (USAR).

With two friendly nations on its northern and southern borders and two large oceans to the east and west, the United States has enjoyed a safe and secure homeland. In the next conflict with a near-peer adversary, the United States should expect enemies can and will engage in all domains within its borders and undertake kinetic attacks on its cities, bases, reserve centers, lines of communication, ports, and airports either by ballistic missile or sleeper cell terrorist attacks. Simultaneous cyber, information, and economic attacks against US critical infrastructure networks and families will occur. The nation will call upon the citizen-soldiers of the reserve component to serve in multiple arenas. As civilians, many reserve component soldiers serve in critical emergency service, medical, and transportation fields. These skills will be in high demand and will compete for reserve component soldiers' priorities in the event the nation is under direct attack. A full mobilization within the context of a contested homeland will stretch the ability of reserve component soldiers to answer the mobilization call.

This appendix focuses on the following questions: What would the impact of full mobilization be on government and private organizations in a contested homeland? What impacts would federal, state, and local governments and private entities experience as key, essential reserve component soldiers are pulled from their organizations and businesses while the homeland is under attack? Finally, what is the impact on the reserve component due to having soldiers whose civilian jobs will be essential? This appendix examines current governmental policies and the potential impacts to the emergency service, transportation, medical, and aviation fields and recommends improvements to the nation's mobilization preparation efforts. It provides a quick, historical review of the US Army Reserve and how it became the "operational reserve" of today's Total Army, outlines the authorities that allow reserve forces to mobilize, and envisions USAR operations in a contested homeland.

HISTORIC CONTEXT

The nation's Founding Fathers recognized the need for a reserve component. In its first century, the United States was a regional power, protected from foreign invasion by the Atlantic and Pacific Oceans. As a result, the federal government chose a military model that funded a very small, professional Army, augmented in times of crisis with militia and volunteer forces. During periods of conflict, the federal government would mobilize a large force of citizen-soldiers and train them before conducting combat operations. After completing these operations, mobilized soldiers would return home.

Although the concept of the National Guard sprang from the tradition of local and state militias, early military leaders such as General George Washington, General Baron von Steuben, General Henry Knox, and General Alexander Hamilton recognized the need for a federal reserve force and proposed its creation.¹ Four significant events in world history shaped the formation of the modern US Army Reserve: the Spanish-American War and Philippine Revolution (1898–1902), World War II (1939–45), the fall of the Berlin Wall and the end of the Cold War (1989), and the war on terrorism (2001–present).²

At the end of the nineteenth century, the United States began to project power outside the continental United States (CONUS) into the Caribbean and Pacific, which ultimately led to the sinking of the USS *Maine* on February 15, 1898, and the beginning of the Spanish-American War and Philippine Revolution. “Mobilization problems of the Army during these conflicts, specifically shortages of medical professionals, trained officers and non-commissioned officers, caused the national leadership to finally establish a formal structure for federal volunteers during peacetime.”³ As a result, Congress created the Medical Reserve Corps in 1908, the predecessor of the Organized Reserve Corps. Subsequently, through the National Defense Acts of 1916 and 1920, the government created the Organized Reserve to provide a peacetime source of trained officers and noncommissioned officers consisting of the officer cadre for up to 27 reserve infantry divisions and six reserve cavalry divisions stationed throughout the country and included the Officer’s Reserve Corps, Enlisted Reserve Corps, and the Reserve Officers’ Training Corps.⁴ This force went on to mobilize almost 90,000 officers and 80,000 enlisted personnel who served in World War I (1917–19). During the interwar years (1920–40), the Army had plans for up to 33 paper or cadre reserve divisions. Although funding and training opportunities for the Organized Reserve were virtually nonexistent, a unique use for the reserve was found when more than 30,000 Organized Reserve Corps officers served as commanders and staff officers in the Civilian Conservation Corps camps between 1933 and 1939.⁵

The closest the United States has come to full mobilization as described by Title 10 of the US Code was World War II; however, the mobilization of Organized Reserve soldiers began before the war started. In 1940, the Organized Reserve Corps began mobilizing for war. In the following year, the number of Organized Reserve Corps officers on duty rose from around 3,000 to more than 57,000.⁶ In 1941–45, the Army mobilized 26 USAR infantry divisions. Over 100,000 Reserve Officers’ Training Corps graduates and over 200,000 Organized Reserve Corps soldiers served during

1. “Brief History of the Army Reserve,” Homeland Security Digital Library (website), n.d., <https://www.hsdl.org/?view&did=437351>, 1.

2. Office of Army Reserve History, *Army Reserve: A Concise History* (Fort Bragg, NC: US Army Reserve Command, 2013), 2.

3. Office of Army Reserve History, *Army Reserve*, 4.

4. Office of Army Reserve History, *Army Reserve*, 4.

5. Office of Army Reserve History, *Army Reserve*, 6.

6. Office of Army Reserve History, *Army Reserve*, 6.

the war.⁷ This mobilization was the largest the US Army Reserve has ever seen, though it would perhaps experience a similar mobilization if the United States were to go to war with a modern, near-peer adversary. Notwithstanding the Pearl Harbor attack and the occupation of several Alaskan islands, the Atlantic and Pacific Oceans have provided the safe haven the United States has required to mobilize the nation's industrial base and deploy military forces. Advances in modern weapons across all military domains suggest the buffers provided by the country's geographic isolation from its near-peer adversaries would not give it the time and space it enjoyed during the full mobilization of World War II.

After World War II, the United States developed a strategy of Soviet containment. For the first time in US history, the nation would require a large, active military force with a robust reserve component to implement a new, global foreign policy. This global foreign policy strategy led to significant changes to the Organized Reserve Corps and began the evolution of the strategic reserve concept.⁸

The Organized Reserve Corps mobilized over 240,000 reservists during the Korean War (1950–53). Based on lessons learned from this large mobilization, Congress enacted several changes to the structure, roles, and authorities of the reserve component. These changes included renaming the Organized Reserve Corps to the US Army Reserve, authorizing 24 inactive and 17 active training days per year, and authorizing the president to mobilize up to one million uniformed personnel from all services to active duty.⁹ After the Korean War, “the Army Reserve was mobilized only twice; over 68,500 Army Reserve Soldiers for the Berlin Crisis (1961–62) and nearly 6,000 for the Vietnam War during the period from 1968 to 1969. In reality, it existed as a strategic reserve.”¹⁰ Operations Desert Shield and Desert Storm—and, to a lesser extent, the short-term contingency operations of the 1990s—validated the strategic reserve model. During Operations Desert Shield and Desert Storm, the US Army Reserve mobilized over 80,000 soldiers to provide combat support and combat service support to the coalition. Subsequently, it provided critical combat support and combat service support during Operation Restore Hope (Somalia), Operation Uphold Democracy (Haiti), Sinai Peninsula peacekeeping operations, and peacekeeping and stabilizing operations in Bosnia and Herzegovina.¹¹

The September 11 attacks ushered in a new century and a fundamental change in the concept of the strategic reserve. The demand for active-duty Army forces and the critical enabling capabilities resident in the reserve component drove the development of the Army Force Generation model. National Guard and USAR units and soldiers were routinely mobilized to serve in the southwest Asia theater of operations, both in Afghanistan and Iraq. In addition to these mobilizations, reserve component soldiers routinely mobilized to serve in the homeland and abroad supporting civil authorities in

7. Office of Army Reserve History, *Army Reserve*.

8. Office of Army Reserve History, *Army Reserve*.

9. Office of Army Reserve History, *Army Reserve*, 10.

10. Office of Army Reserve History, *Army Reserve*, 11.

11. Office of Army Reserve History, *Army Reserve*, 14–15.

humanitarian assistance and disaster relief operations. Sixteen years of persistent combat operations in Afghanistan and Iraq, as well as defense support of civil authorities (DSCA) requirements, have transformed the US Army Reserve into an operational reserve.¹² The active component of the Army depends on reserve component soldiers to provide critical enabling capabilities that are sparse in the active component. The US Army Reserve possesses over 50 percent of the Total Army's capacity in many specialties, including medical support, quartermaster, chaplain, military information support operation, and civil affairs.¹³

In addition to supporting the active component in overseas contingency operations around the world, the US Army Reserve has increasingly supported DSCA operations in the continental United States. Under authorizations provided by the 2018 revision of the Stafford Act (Disaster Recovery Reform Act), the US Army Reserve can provide federal assistance to civil authorities after a state governor has requested assistance and the president has made a disaster declaration. Additionally, under DoD Directive 3025.18, USAR commanders may take action to "save lives, prevent human suffering, or mitigate great property damage in response to a request for assistance from a civil authority, under imminently serious conditions."¹⁴ The US Army Reserve also maintains a standing task force available for immediate mobilization and deployment in the event of a chemical, biological, radiological, nuclear, or explosives attack.¹⁵ Based on these authorizations, the US Army Reserve has become increasingly important in the *National Response Framework* (NRF) plans to combat natural and manmade disasters within the United States.

CONTESTED HOMELAND

In their 2015 book *Ghost Fleet*, P. W. Singer and August Cole present a vision of a current-day war between the United States and a coalition consisting of China and Russia. Though the book can be overly dramatic, its portrayal of a US war with a near-peer competitor is very realistic. The authors vividly describe a scenario in which a massive strike in the space and cyber domains cripples the US military's technical dominance. In a matter of hours, the United States' space-based Global Positioning System (GPS); communication; intelligence, surveillance, and reconnaissance; and weather satellites are taken out of commission through a combination of terrestrial and ground-based, anti-satellite systems. Simultaneously, the coalition attacks the United States' civil and

12. Office of Army Reserve History, *Army Reserve*, 12, 15.

13. "Indispensable Capabilities for the Operational Force," <https://www.usar.army.mil/Portals/98/Documents/infographics/MOS%20Breakdown.pdf?ver=2015-10-29-113631-337>, US Army Reserve (website), n.d., <https://www.usar.army.mil/News/Infographics/>.

14. William J. Lynn III, *Defense Support of Civil Authorities*, DoD Directive 3025.18 (Washington, DC: Under Secretary of Defense for Policy, updated March 19, 2018), 18.

15. HQDA, *Chemical, Biological, Radiological, Nuclear, and Explosives Command*, Army Techniques Publication 3-37.11 (Washington, DC: HQDA, August 2018); and US Army Reserve Specialized Disaster Response Forces, "CRE: An Army Reserve Reference Guide," US Army Reserve (website), n.d., <https://www.usar.army.mil/Portals/98/Documents/Ambassadors/Chemical%20Response%20Enterprise%20Brochure.pdf>.

military systems with massive cyberattacks.¹⁶ The authors do, however, omit some events that could occur within the continental United States should this type of conflict happen. Over the past 30 years, potential adversaries of the United States have been observing its operations in Kuwait, Iraq, and Afghanistan and its large-scale withdrawal from forward basing in Europe.¹⁷ These operations could be characterized as operations in which the United States was able to conduct large-scale mobilizations and deployments from the continental United States to staging bases near the areas of operations unmolested by adversaries. If a near-peer competitor were entering into conflict with the United States, allowing the United States to mobilize its Total Force and deploy from the continental United States to forward staging bases near the area of operations would be a strategic mistake. The near-peer competitor of the future will attack the United States across multiple domains and within the homeland.¹⁸ In the United States' next major war, the homeland will be contested.

A contested homeland would severely test the ability of the Total Force to alert, mobilize, organize, and deploy to the area of operations. Reserve component soldiers of all types would be heavily involved in reacting to attacks on the homeland, in both their civilian and military roles. *Ghost Fleet* and several recent articles describe in depth potential, national vulnerabilities in the space, cyber, and information domains. Space-based GPS; intelligence, surveillance, and reconnaissance; and communications assets are vulnerable to kinetic and electromagnetic attacks and cyberattacks. Losing these assets would greatly reduce capabilities across all segments of American society, complicating the command and control of the Total Force. Nowhere would this loss of command and control be felt greater than in the execution of a total or full mobilization under 10 US Code section 12301(a) or section 12302.

Cyberattacks would likely target critical government and business systems. The federal government has previously recognized these vulnerabilities. President Bill Clinton issued Presidential Decision Directive 63 on critical infrastructure protection in 1998. This directive was updated by President George W. Bush with Homeland Security Presidential Directive 7 in 2003.¹⁹ An attack on critical and vulnerable infrastructure segments could lead to infrastructure failures in commerce and banking, transportation systems (air and sea traffic, public transportation, and transportation infrastructure), energy (electrical power and the production, refining, storage, and distribution of oil and gas), public health (health care and agriculture), environmental protection (drinking water, water treatment, and hazardous waste storage), and government

16. P. W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War* (Boston: Houghton Mifflin Harcourt, 2015), 1-4.

17. Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessments, 2003).

18. Kevin D. Scott, *Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: Joint Chiefs of Staff, July 14, 2016), 24-27.

19. William J. Clinton, *Critical Infrastructure Protection*, Presidential Decision Directive/National Security Council 63 (Washington, DC: White House, May 22, 1998); and George W. Bush, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (Washington, DC: White House, December 17, 2003).

(continuity of government, the defense industrial base, law enforcement, emergency management, and state and local government).²⁰

Although the cyberattacks and space attacks on the nation's infrastructure described in *Ghost Fleet* would wreak havoc, kinetic attacks on the homeland, would be more damaging to the reserve component's ability to mobilize. In the event of conflict with China or Russia, the dilemma facing the United States would center on its Joint Force gaining access to Asia and Europe. This dilemma is based on potential adversaries' development and deployment of sophisticated anti-access/area-denial (A2/AD) systems in both theaters. Most of the current A2/AD discussion centers on defensive tactics are designed to limit the US Joint Force's access to aerial ports and seaports of debarkation in Europe and Asia.²¹ Sophisticated, defensive, ballistic missile defense and air defense systems and offensive, land- and sea-launched, ballistic missile systems are described in detail as denial mechanisms to keep the US Joint Force out of theater. In the author's opinion, adversaries with these sophisticated systems and capabilities would not limit their attacks on the US homeland to the space and cyber domains. These adversaries would attack US infrastructure, ports of embarkation, and military forces in the homeland. The adversaries would attack across all domains to prevent the United States from mobilizing and deploying outside the continental United States. Kinetic attacks in the land, sea, and air domains would target and disrupt the United States' unmatched capability to mobilize and project power from home. The most likely course of action for a near-peer adversary would be to insert special operations forces into the United States preconflict to attack select military and civil infrastructure targets on order.

Near-peer competitors also have air- and sea-based missile systems that could maneuver into range to attack critical targets in the United States. As noted by Ian Williams in "The Russia-NATO A2AD Environment," a critical component of NATO's ability to support alliance members is a series of aerial ports and seaports of debarkation within the Russian A2/AD envelope.²² "Disabling these nodes would complicate NATO's ability to efficiently respond to crisis."²³ China is currently extending its A2/AD capability through system development and expansion into the South China Sea.²⁴ Aerial ports and seaports of embarkation in the United States are as critical as aerial ports and seaports of debarkation in theater. An adversary using cyberattacks, special operations forces, and missile attacks on the aerial ports and seaports of

20. Clinton, *Critical Infrastructure Protection*.

21. Ian Williams, "The Russia-NATO A2AD Environment," Missile Threat, CSIS Missile Defense Project (website), January 3, 2017, <https://missilethreat.csis.org/russia-nato-a2ad-environment/#en-1298-2>.

22. Williams, "Russia-NATO A2AD Environment."

23. Williams, "Russia-NATO A2AD Environment."

24. Christopher Cowan, "A2/AD—Anti-Access/Area Denial," RealClearDefense (website), September 12, 2016, https://www.realcleardefense.com/articles/2016/09/13/a2ad_-_anti-accessarea_denial_110052.html; and David McDonough, "China's Naval Strategy—from Sea Denial to Sea Control?," Australian Strategic Policy Institute Strategist (website), August 1, 2013, <https://www.aspistrategist.org.au/chinas-naval-strategy-from-sea-denial-to-sea-control>.

mbarkation within the continental United States would delay deploying forces and cause casualties, damage, and confusion throughout the country. These attacks would divert critical government and civilian assets away from the already difficult task of mobilizing and deploying the Total Force outside the United States.

WHAT IS MOBILIZATION?

Mobilization, as defined by the Department of Defense, “is the process of assembling and organizing national resources to support national objectives in time of war or other emergencies.”²⁵ The authorities for mobilizing the national resources are enshrined in the Constitution of the United States of America, which states the following in article 1, section 8:

The Congress shall have power . . . [t]o provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions; To provide for organizing, arming, and disciplining the Militia, and for governing such part of them as may be employed in the Service of the United States, reserving to the States respectively, the Appointment of the officers, and the Authority of training the Militia according to the discipline prescribed by Congress.²⁶

Title 10 of the US Code defines the different levels of mobilization, from voluntary call to total, national mobilization.²⁷ Each level of mobilization is characterized by emergency authority, level of military commitment, and length of mobilization.²⁸ The partial mobilizations are limited in both duration and level of commitment. If the president were to mobilize the reserve component, as authorized by 10 US Code, section 12304, a maximum of 200,000 Selected Reserve soldiers, including up to 30,000 Individual Ready Reserve soldiers, could be mobilized for up to 365 days. This emergency authority may be delegated to the secretary of defense.²⁹ Federal reserve component soldiers mobilized under this section may be used either to support the states in a disaster relief effort for up to 120 days (section 12304[a]), as described in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 US Code, section 5122), or to support a combatant commander in a given operation for up to 365 days (section 12304[b]).³⁰ Another level of mobilization short of full mobilization is partial mobilization, which is enacted with a presidential declaration of national emergency per

25. Daniel O’Donohue, *Joint Mobilization Planning*, Joint Publication 4-05 (Washington, DC: Joint Chiefs of Staff, October 23, 2018), I-1.

26. US Constitution Article I, Section 8.

27. Reserve Components Generally, 10 US Code Section 12301 (2004); Ready Reserve, 10 US Code Section 12302 (2011); Ready Reserve: Members Not Assigned to, or Participating Satisfactorily in, Units, 10 US Code, Section 12303 (1994); and Selected Reserve and Certain Individual Ready Reserve Members; Order to Active Duty Other Than during War or National Emergency, 10 US Code, Section 12304 (2018).

28. Ken S. Gilliam and Barrett K. Parker, “Mobilization: The State of the Field,” *Parameters* 47, no. 2 (Summer 2017).

29. Selected Reserve and Certain Individual Ready Reserve Members.

30. Selected Reserve and Certain Individual Ready Reserve Members.

10 US Code, section 12302. Not more than one million Ready Reserve members can be mobilized on active duty for up to 24 months without their consent at any one time.³¹

In the event of a full-scale conflict with a near-peer adversary, the president would most likely use 10 US Code, Section 12302, in conjunction with a presidential declaration of national emergency to initiate a full mobilization of the Total Army. Mobilization of the Total Army under Section 12302 would exclude members of the standby reserve and the retired reserve.³² Most likely, a Congressional declaration of war would follow, authorizing a full mobilization of the reserve component. Under Section 12301(a), the President or another authority designated by the secretary of the military branch being mobilized may order any member of the selected reserve, including standby reserve and retired reserve members, to active duty for the duration of the war or national emergency.³³ In the event the secretary of the branch being mobilized determines the reserve does not have enough active members with the requisite skill sets, the secretary, with the approval of the Secretary of Defense, may recall inactive and retired reserve members to active duty.³⁴ The authorizations contained in Section 12301(a) and the associated mobilization levels of the reserve component have not been used since the total mobilization of World War II.³⁵ See figure B-1 for a depiction of the levels of mobilization.

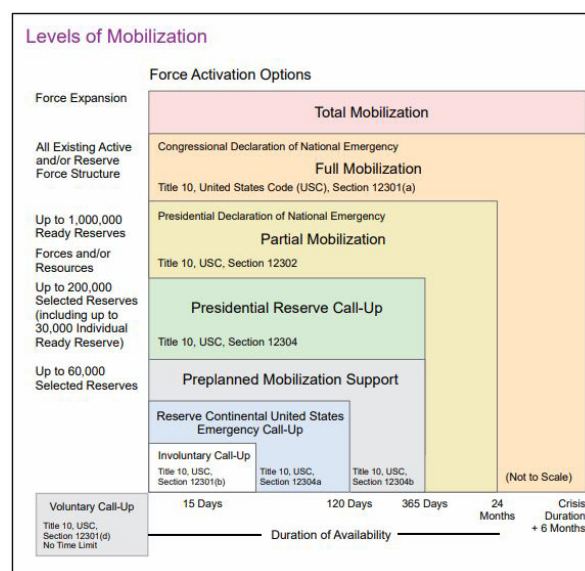


Figure B-1. Levels of mobilization

31. Ready Reserve.

32. School of Strategic Landpower, *How the Army Runs 2015–2016: A Senior Leader Reference Handbook* (Carlisle, PA: US Army War College Press, 2015), 6-3–6-4, 6-10.

33. Reserve Components Generally; and School of Strategic Landpower, *How the Army Runs*, 6-10.

34. Reserve Components Generally.

35. O'Donohue, *Joint Mobilization Planning*.

Because mobilization of the reserve component as part of the Total Force is so critical to the National Defense Strategy of the nation, the Department of Defense has established several policies to ensure the component is available to the department. Because the nation has only used limited mobilizations since World War II, leaders with full reserve component mobilization experience have long since retired from the force. To ensure mission success in the event of a declared war or national emergency, full mobilization should be exercised at multiple levels. In fact, DoD policy states, “Mobilization exercises are conducted in conjunction with Military Service, joint, and CCMD exercises so that RC access policy and procedures are regularly exercised, practiced, and understood throughout the force. Pursuant to section 10208 of Reference (d), the Secretary of Defense will conduct at least one major mobilization exercise each year.”³⁶

Despite this requirement, the Department of Defense and, to some extent, the services are not currently satisfying this requirement at the level of full or total mobilization.

GAPS IN FULL MOBILIZATION PLANNING, EXERCISES, AND REGULATIONS

Joint Publication 4-05, *Joint Mobilization Planning*, promulgates guidance to be used by the armed forces in preparing their mobilization plans.³⁷ This publication prescribes the roles and responsibilities for the planning and execution of mobilization. The Joint planning and execution community collectively plans for the mobilization and deployment of the Joint Force.³⁸ In addition to Joint Staff and service mobilization planning, supporting US government agencies should conduct planning and coordination activities to mobilize the national support base to sustain the fully mobilized Joint Force.³⁹ As part of the Joint planning and execution community, the Joint Staff Logistics Directorate is the focal point for the integration of planning and coordination of mobilization execution. The services are responsible for preparing detailed mobilization plans, identifying the forces and support to be provided, and executing mobilization at the direction of the Secretary of Defense.⁴⁰ Based on several telephone conversations with representatives of the Office of the Secretary of Defense, Joint Staff, and Department of the Army mobilization representatives, the last DoD-wide mobilization exercise occurred in 1982, before the commissioning of most senior Army leaders.⁴¹ In 1978, the Department of Defense conducted Exercise Nifty Nugget, which

36. Peter Levine, *Accessing the Reserve Components (RC)*, DoD Instruction 1235.12 (Washington, DC: Office of the Secretary of Defense, updated February 28, 2017), 2.

37. O'Donohue, *Joint Mobilization Planning*.

38. O'Donohue, *Joint Mobilization Planning*.

39. O'Donohue, *Joint Mobilization Planning*.

40. O'Donohue, *Joint Mobilization Planning*.

41. Victor Parziale, Office of the Under Secretary for Personnel and Readiness, interview by the author, February 2, 2018; Aaron Angell, Joint Chiefs of Staff Logistics, interview by the author, February 5, 2018; and Charles Wack, HQDA Operations, interview by the author, February 14, 2018.

was followed by Exercise Proud Spirit in 1980 and Exercise Proud Saber in 1982.⁴² These exercises were based on a hypothetical war with Soviet Union and Warsaw Pact forces in Europe. Rather than focusing on multicomponent personnel mobilization issues, Exercise Proud Spirit and Exercise Proud Saber focused on:

- assessing the interface among the Office of the Secretary of Defense, the Joint Staff, federal agencies (the Federal Emergency Management Agency), the Army, and other services;
- assessing plans to facilitate and support the mobilization, deployment, and sustainment of the reserve component;
- evaluating the capabilities of the CONUS support base to expand and support mobilization;
- evaluating the capability of the automated data processing system to support mobilization and deployment; and
- evaluating the ability of command-and-control systems and communications to support the planning and execution of mobilization and deployment.⁴³

In recent years, the Army has begun to focus more time and effort on studying mobilization issues. Several recent tabletop exercises have been conducted, beginning in 2016. Each of these tabletop exercises, however, have focused primarily on one region's operations plan and time-phased force and deployment data.⁴⁴ Although these tabletop exercises have generated discussion across the DoD enterprise, as of 2021, Headquarters, Department of the Army has not exercised a full mobilization of the entire reserve component, nor does it plan to in the near future.⁴⁵

WHAT WE DO NOT KNOW MIGHT HURT US

In addition to the lack of comprehensive, Joint mobilization exercises, the US Army Reserve suffers from a critical information deficit. Current USAR personnel systems do not adequately provide senior USAR leaders with high-fidelity employment information on their Ready Reserve soldier population. At this time, US Army Reserve Command (USARC) does not possess a repository of historical or current data on the civilian positions its soldiers occupy outside the Army.⁴⁶ Additionally, it does not have policies in place that address potential conflicts between the US Army Reserve and civilian

42. James W. Canan, "Up from Nifty Nugget," *Air Force Magazine* (website), September 1, 1983, <https://www.airforcemag.com/article/0983nifty/>.

43. Office of the Deputy Chief of Staff for Operations and Plans, *Exercise Proud Spirit/MOBEX 80 After-Action Report* (Washington, DC: HQDA, June 1981), I-3.

44. Charles Wack, interview by the author.

45. Charles Wack, interview by the author.

46. Lee Gearhart, US Army Reserve Command, interview by the author, December 5, 2017, and January 17–18, 2018.

jobs during a full mobilization.⁴⁷ Army Regulation 135-133, *Ready Reserve Screening, Qualification Records System, and Change of Address Reporting*, provides guidance on “key positions” in the federal government that disqualify soldiers from serving in the Ready Reserve.⁴⁸ The regulation also provides procedures for federal agencies to declare reserve component soldiers as holding key positions and to request the soldiers be transferred to the Standby Reserve.⁴⁹ Figure B-2 shows the federal key-position memorandum.

 **DEPARTMENT OF THE ARMY**
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

From: **(Employer-Agency or Company)**

To: Commander, U.S. Army Human Resources Command (AHRC-OPL-P), 1600 Spearhead
Division Avenue, Fort Knox, KY 40122-5208

Subject: Request for Employee to be Removed from the Ready Reserve

This is to certify that the employee identified below is vital to the nation's defense efforts in **(his or her)** civilian job and cannot be mobilized with the Military Services in an emergency for the following reasons:

(List reason(s))

Therefore, I request that **(he or she)** be removed from the Ready Reserve and that you advise me accordingly when this action has been completed.

The employee is:

1. Name of employee **(last, first, M.I.)**:
2. Military grade and Reserve component:
3. Social security number:
4. Current home address **(street, city, State, and ZIP code)**:
5. Military unit to which assigned **(location and unit number)**:
6. Title of employee's civilian position:
7. Grade or salary level of civilian position:
8. Date (YYMMDD) hired or assigned to position:

(Signature and Title of Agency or
Company Official)

Figure B-2. Federal key position memorandum

Similar data is not required to be collected for reserve component soldiers occupying key positions in state and local government or critical civilian industries.⁵⁰ The regulation only encourages nonfederal employers of Ready Reserve soldiers to “adopt personnel management procedures designed to preclude conflicts between

47. Lee Gearhart, interview by the author.

48. HQDA, *Ready Reserve Screening, Qualification Records System, and Change of Address Reporting*, Army Regulation 135-133 (Washington, DC: HQDA, October 3, 2019).

49. HQDA, *Ready Reserve Screening*.

50. HQDA, *Ready Reserve Screening*.

emergency manpower needs of civilian employment activities and the military during a mobilization” and encourages Ready Reserve soldiers “to use the Federal key positions guidelines contained herein for making their own key position designations and, as applicable, recommending key employees for removal from the Ready Reserve.”⁵¹ Because it does not mandate screening below the federal government level, the US Army Reserve lacks important data on its soldier population. This absence of critical information could lead to false assumptions and planning gaps in the event a full mobilization is ordered.

The US Army Reserve currently uses three systems or databases to track personnel—the Regional Level Application Software (RLAS); the Total Army Personnel Database – Reserve, which is fed by RLAS; and the Commander’s Strength Management Module.⁵² US Army Reserve commanders, unit administrators, and soldiers are relied on to update the systems annually. This reporting mechanism is widely underused, and, even when the information in the systems is up to date, it does not provide USAR leadership with enough detail.⁵³ Although RLAS currently tracks over 900 job descriptions, the detail USAR leaders and mobilization planners require is still lacking. The job descriptors in the systems are overly broad and do not indicate whether a job is a critical civilian or government job that would be in demand during a full mobilization in a contested homeland. For example, though “police officer” and “sheriff” are provided as options, the system does not allow for Ready Reserve members to indicate whether they are local, county, state, or federal law enforcement officers or specify the agency or organization for which they work. Other critical government positions that do not show appropriate levels of specificity within RLAS include chief elected or appointed officials, emergency managers, legislators or executive branch officials, emergency medical services, firefighters, public health officials, intelligence analysts, and cyber practitioners. Similar issues exist in critical civilian industries, such as health care, transportation, engineering, logistics and supply chain management, and power generation and distribution. By not drilling down to the necessary level of specificity, USAR and mobilization planners at the Army and Joint level cannot anticipate potential conflicts between reserve mobilization and civilian demands at the soldier or unit level, especially while the homeland is under attack.

RECOMMENDATIONS

At the beginning, this appendix posed some questions: What would the impact of full mobilization be on government and private organizations in a contested homeland? What impacts would federal, state, and local governments and private entities experience as key and essential reserve component soldiers were pulled from their organizations and businesses while the homeland is under attack? First, to answer these questions, the Department of Defense must exercise full mobilization in a contested homeland scenario. It is currently not fulfilling its obligation under Title 10 of US Code

51. HQDA, *Ready Reserve Screening*.

52. Yolanda Jones, interview by the author, February 1–2, 2018.

53. Lee Gearhart, interview by the author.

and DoD Instruction 1235.12. Until the Department of Defense fulfills this obligation, the United States will not be able to demonstrate the US Army Reserve will be able to meet its mobilization obligation to the nation during a full mobilization. Due to the massive scope of this undertaking, the DoD response to this requirement should take an incremental approach until compliance has been achieved. First, the individual services should exercise full mobilization of the reserve component. Once exercises have been accomplished at the service level, the Department of Defense should then exercise full mobilization. The next step would be to exercise full mobilization under a contested homeland scenario. As the complexity of the mobilization exercises increases, a whole-of-government approach should be exercised. This approach would exercise elements of civilian industry, the Joint Force, and interagency and intergovernmental partners. Finally, since the worst-case scenario for a near-peer attack would occur as mobilized elements of the reserve component were assisting civil authorities following a natural or man-made disaster, simulations should exercise the friction points and conflicts that may occur among reserve component soldiers, their civilian occupations, and National Guard obligations during state-level response. In the exercise, the Federal Emergency Management Agency should be responsible for disaster response within the homeland, and key government and civilian partners should be invited to participate as well. One of the objectives of this exercise should be to stress the national response to both nonkinetic and kinetic attacks to cyber systems, national transportation hubs and infrastructure, and power grids as the reserve component is called to full mobilization.

Second, US Army Reserve Command must fix its dangerous personnel information gap. The command currently lacks vital data on Ready Reserve soldiers serving in critical civilian professions.

Given its lack of civilian employment data on its soldiers, the US Army Reserve has no concept of the potential impacts of full mobilization in a contested homeland at this time. It should update Army Regulation 135-133 to mandate that each Ready Reserve soldier identify his or her civilian position in RLAS and the Integrated Personnel and Pay System, the USAR personnel databases of record. This requirement should be conducted annually, at a minimum. The priority of effort is to capture Ready Reserve member information and then expand to the standby reserve and retired reserve members. As part of this effort, civilian occupation codes in RLAS must be updated to identify critical government and civilian positions in greater detail. Information on critical federal, state, and local government positions that may conflict with the US Army Reserve during full mobilization must be captured. Critical government positions include chief elected or appointed officials, emergency managers, legislators or executive branch officials, law enforcement, emergency medical services, firefighters, public health officials, intelligence analysts, and cyber practitioners. In addition to government positions, US Army Reserve Command should capture data on critical civilian positions, including medical providers, transportation employees, engineers, logistics and supply-chain managers, and power-generation and distribution workers. The US Army Reserve can never fully understand the potential impacts and friction points of a full mobilization in a contested homeland until it knows which soldiers work in these critical government and civilian positions.

Finally, the US Code and certain DoD directives and instructions and Army regulations should be revised to compel the collection of information on reserve component soldiers' employment. Department of Defense Directive 1200.7 was written in November 1999 and certified as current in November 2003.⁵⁴ Since then, the Total Army's dependence on the reserve component has increased, and the US Army Reserve has transitioned from a strategic reserve to an operational one.⁵⁵ The directive is long overdue for an update. As part of this revision, 10 US Code, Section 10149, "Ready Reserve: Continuous Screening," should be updated to codify the closing of the knowledge gap highlighted earlier. In addition, the US Army Reserve should examine increasing Individual Mobilization Augmentation and Individual Ready Reserve mobilization options to increase the available Ready Reserve force in the event of a full mobilization. Finally, Army Regulation 135-133 should be revised to provide USAR commanders with guidance on identifying and tracking Ready Reserve soldiers who occupy critical government and civilian positions and are not currently designated as such in the system. The regulation currently addresses reserve soldiers who are disqualified from serving in the Ready Reserve because of the nature of their civilian jobs.⁵⁶ The regulation should be amended to include the identification of reserve soldiers who serve in critical positions but do not meet the current threshold for disqualification. These modifications to the US Code, DoD policy, and Army regulations would help the Total Force anticipate potential job conflicts in the reserve component during total mobilization.

CONCLUSION

In conclusion, the complete impact of a full mobilization on government and civilian organizations and the impact of reserve soldiers serving in critical government and civilian occupations on mobilization rates are currently unclear. Although the likelihood of a conflict with a near-peer adversary may seem low, the United States, in today's volatile and uncertain geopolitical landscape, must prepare for the worst-case scenario. The consensus seems to be in the event of a national declaration of war or a presidential declaration of national emergency that requires the use of Section 12301(a) or Section 12302 mobilization authorizations, the federal mobilization effort would trump any other concern. Believing all reserve component soldiers will be able to immediately walk away from their civilian professions to answer the call is naive. In some instances, reserve component soldiers should perhaps temporarily delay their mobilization to continue to serve in their civilian roles. First, the entire Joint planning and execution community must begin to study and exercise full mobilization scenarios using a whole-of-government approach to understand fully any potential shortcomings in the nation's response in this dangerous scenario.

54. John J. Hamre, *Screening the Ready Reserve*, DoD Directive 1200.7 (Washington, DC: OSD, November 18, 1999).

55. Eric P. Samaritoni, *Problems with Transitioning the US Army Reserve (USAR) from a Strategic to an Operational Reserve Force* (Fort Leavenworth, KS: US Army Command and General Staff College, 2018), iii.

56. HQDA, *Ready Reserve Screening*.

Additionally, the US Code and DoD directives and instructions should be updated to address these situations. The type of citizens who volunteer to serve in the reserve component of the military are the same types of citizens who serve in key government and private sector positions. These citizens serve and manage the nation and their local communities. When the nation is attacked, these citizen-soldiers will be on the front lines in their communities as first responders and medical providers, repairing damage and bringing infrastructure and services back online for their states and communities. Because it does not currently track the critical civilian professions its citizen-soldiers occupy to the degree it should, the reserve component cannot fully understand the potential friction and conflicts that may occur between the dual roles its members might be expected to inhabit during full mobilization.

APPENDIX C ACRONYMS AND ABBREVIATIONS

A2/AD	Anti-Access/ Area Denial
ADP	Army Doctrine Publication
APP	Army Protection Program
ASCE	American Society of Civil Engineers
CONUS	Continental United States
CRR	Cyber Resilience Review
DCMA	Defense Contract Management Agency
DHS	Department of Homeland Security
DoD	Department of Defense
DSCA	Defense Support of Civil Authorities
EMP	Electromagnetic Pulse
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
GAO	Government Accountability Office
GPS	Global Positioning System
HQDA	Headquarters, Department of the Army
IT	Information Technology

JTF	Joint Task Force
LFA	Lead Federal Agency
LOE	Line of Effort
MDO	Multi-domain Operations
MOTCO	Military Ocean Terminal Concord
MOTSU	Military Ocean Terminal Sunny Point
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NMT	National Mission Team
NNEMP	Nonnuclear Electromagnetic Pulse
NPS	National Preparedness System
NRF	National Response Framework
OSD	Office of the Secretary of Defense
PPD	Presidential Policy Directive
RLAS	Regional Level Application Software
ROC	Rehearsal of Concept
SAD	State Active Duty
SDDC	Military Surface Deployment and Distribution Command

SLTT	State, Local, Tribal, and Territorial
SSA	Strategic Support Area
STRAHNET	Strategic Highway Network
TEA	Transportation Engineering Agency
UCG	Cyber Unified Coordination Group
USAR	US Army Reserve
USCG	US Coast Guard
USCYBERCOM	US Cyber Command

ABOUT THE RESEARCHERS

PROJECT DIRECTORS

Professor Bert B. Tussing is the director of the Homeland Defense and Security Issues Group at the US Army War College Center for Strategic Leadership. He holds a bachelor's degree in English from The Citadel and master's degrees in national security and strategic studies from the US Naval War College and in strategic studies from the US Army War College. He is a distinguished graduate of the Marine Corps Command and Staff College.

Dr. John Eric Powell is a visiting professor assigned to the US Army War College as the liaison officer from the Homeland Defense Civil Support Office at the Maneuver Support Center of Excellence at Fort Leonard Wood. He holds bachelor of science degrees from Western Carolina University and Colorado State University; master's degrees from the Medical University of South Carolina, the Naval Postgraduate School, and the University of South Florida; and a doctorate from the University of Tennessee at Knoxville.

Colonel Benjamin C. Leitzel, US Air Force retired, is a professor at the US Army War College, where he oversees senior leader cyberspace education and leads the college's cyber working group.

CONTRIBUTING RESEARCHERS

Colonel Jonathan M. Boling, a US Air Force cyberspace operations officer assigned to the Defense Information Systems Agency, holds a bachelor's degree from the Virginia Polytechnic Institute and State University, a master's degree in information technology from the University of Maryland Global Campus, and a master's degree in strategic studies from the US Army War College.

Colonel James L. (Jim) Boling, US Army retired, holds a master's degree in political science from the University of Louisville and master's degrees in strategic studies from the US Army War College, in military arts and sciences from the US Army Command and General Staff College, and in national security and strategic studies from the US Naval War College (*magna cum laude*). He is a graduate of the US Army War College Advanced Strategic Arts Program and the US Army Command and General Staff College School of Advanced Military Studies.

Dr. John J. Borek is a postdoctoral fellow with the US Army War College Homeland Defense and Security Issues Group. He holds a bachelor of science degree in geography from the Pennsylvania State University, a master's degree in strategic intelligence from the National Intelligence University, and a PhD in public policy from Walden University. He is also an adjunct professor with the University of New Hampshire National Security Intelligence Analysis program.

Mr. Charles “Chuck” P. Brady works in the Operations Department of the Defense Threat Reduction Agency. He holds a bachelor’s degree in business from the University of Notre Dame, a master’s degree in business administration from Webster University, and a master’s degree in national security strategy from the US Army War College. He is also a graduate of the Marine Corps Command and Staff College.

Colonel John Bretthorst, a US Army logistics officer currently assigned as the Chief of Staff of the US Army Physical Disability Agency, Joint Base San Antonio, holds a master’s degree in strategic studies from the US Army War College and bachelor’s and master’s degrees in history from Tarleton State University.

Colonel Stephen W. Ladd, a US Army aviator assigned to US Army Reserve Aviation Command at Fort Knox, holds a bachelor’s degree from the United States Military Academy and a master’s degree in strategic studies from the US Army War College.

Colonel Steven E. Landis, US Army retired, held a bachelor’s degree in political science from Duke University and a master’s degree in security studies from the US Army War College. Landis passed away in July 2020.

Colonel Edmund “Beau” Riely holds a bachelor’s degree in finance from Georgetown University, a master’s degree in business administration from the University of Maryland, and a master’s degree in strategic studies from the US Army War College.

Colonel Arthur C. Roscoe, a US Army logistics officer assigned to the New Jersey Army National Guard as Deputy Chief of Staff, G-4, holds a bachelor’s degree from Rutgers University and a master’s degree in strategic studies from the US Army War College.

Colonel Brian D. Wisniewski, US Army Reserve, is currently assigned to the Army Reserve Innovation Command as the G-2 and G-6. In his civilian employment, he is an operations manager for the NASA Office of Cybersecurity Services. He holds a bachelor’s degree from the University of Toledo, a master’s degree from Webster University, and a master’s degree in strategic studies from the US Army War College.

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College at this time in our nation's history is to produce graduates who are skilled critical thinkers and complex problem solvers in the global application of Landpower. Concurrently, it is our duty to the Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate on ground forces' role in achieving national security objectives.



The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The SSI Live Podcast Series provides access to SSI analyses and scholars on issues related to national security and military strategy with an emphasis on geostrategic analysis. <https://ssi.armywarcollege.edu/ssi-live-archive>



The Center for Strategic Leadership provides strategic education, ideas, doctrine and capabilities to the Army, the Joint Force, and the Nation. The Army, Joint Force, and National partners recognize CSL as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.change through evidence-based decision making.



The School of Strategic Landpower provides support to the USAWC purpose, mission, vision, and the academic teaching departments through the initiation, coordination, and management of academic related policy, plans, programs, and procedures, with emphasis on curriculum development, execution, and evaluation; planning and execution of independent and/or interdepartmental academic programs; student and faculty development; and performance of academic related functions as may be directed by the Commandant.



The US Army Heritage and Education Center makes vailable contemporary and historical materials related to strategic leadership, the global application of Landpower, and US Army Heritage to inform research, educate an international audience, and honor soldiers, past and present.



The Army Strategic Education Program executes General Officer professional military education for the entire population of Army General Officers across the total force and provides assessments to keep senior leaders informed and to support programmatic change through evidence-based decision making.

US ARMY WAR COLLEGE
Major General David C. Hill
Commandant

STRATEGIC STUDIES INSTITUTE

Director
Dr. Carol V. Evans

Director of Strategic Research
Colonel George Shatzer

US ARMY WAR COLLEGE PRESS

Editor in Chief
Dr. Antulio J. Echevarria II

Digital Managing Editor
Mr. Richard K. Leach

Managing Editor
Ms. Lori K. Janning

Developmental Editors
Dr. Erin M. Forest
Dr. Joe Hadley

Visual Information Specialists
Ms. Kristen G. Taylor
Ms. Stephanie Crider

Composition
Mrs. Jennifer E. Nevil



<https://press.armywarcollege.edu>

