

PERSPECTIVES ON CYBER POWER



CPP-7

# US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure

Scott A. Weed  
Major, USAF



AIR FORCE RESEARCH INSTITUTE PAPERS

**Air University**

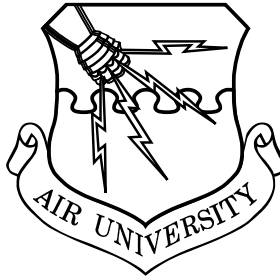
Steven L. Kwast, Lieutenant General, Commander and President

**Air Force Research Institute**

Dale L. Hayden, PhD, Director

**AIR UNIVERSITY**

**Air Force Research Institute  
Perspectives on Cyber Power**



**US Policy Response to Cyber Attack  
on SCADA Systems Supporting Critical  
National Infrastructure**

SCOTT A. WEED  
Major, USAF

CPP-7

Air University Press  
Air Force Research Institute  
Maxwell Air Force Base, Alabama

*Project Editor*  
James S. Howard

*Copy Editor*  
Carolyn Underwood

*Cover Art, Book Design, and Illustrations*  
Daniel Armstrong

*Composition and Prepress Production*  
Vivian D. O'Neal

*Print Preparation and Distribution*  
Diane Clark

---

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

*Director and Publisher*  
Dale L. Hayden, PhD

*Editor in Chief*  
Oreste M. Johnson

*Managing Editor*  
Dr. Ernest Allan Rockwell

*Design and Production Manager*  
Cheryl King

Air University Press  
600 Chennault Circle, Building 1405  
Maxwell AFB, AL 36112-6010  
e-mail: [afri.aupress@us.af.mil](mailto:afri.aupress@us.af.mil)

<http://www.au.af.mil/au/aupress>

Facebook:  
<https://www.facebook.com/AirUnivPress>  
and

Twitter: <https://twitter.com/aupress>



## Library of Congress Cataloging-in-Publication Data

Names: Weed, Scott A., 1979- author. | Air University (U.S.). Air Force Research Institute, issuing body.  
Title: US policy response to cyber attack on SCADA systems supporting critical national infrastructure / Scott A. Weed.  
Other titles: U.S. policy response to cyber attack on SCADA systems supporting critical national infrastructure | United States policy response to cyber attack on SCADA systems supporting critical national infrastructure | Air Force Research Institute perspectives on cyber power ; CPP-7. 2329-5821  
Description: Maxwell Air Force Base, Alabama : Air University Press, Air Force Research Institute, [2017] | Series: Air Force Research Institute perspectives on cyber power, ISSN 2329-5821 ; CPP-7 | Includes bibliographical references and index.  
Identifiers: LCCN 2017012890 | ISBN 9781585662760  
Subjects: LCSH: Computers—Access control—Government policy—United States. | Supervisory control systems—Security measures—United States. | Cyberterrorism—Prevention. | Computer security—Government policy—United States. | Computer security—International cooperation. | Cyberinfrastructure—Security measures—United States.  
Classification: LCC QA76.9.A25 W4255 2017 | DDC 005.8/3—dc23 | SUDOC D 301.26/31:7  
LC record available at <https://lccn.loc.gov/2017012890>  
Published by Air University Press in May 2017

## Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air Force Research Institute, Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

### Air Force Research Institute Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Air Force Research Institute studies are available via the AU Press website at <http://www.au.af.mil/au/aupress/papers.asp>. Please submit comments to [afri.aupress@us.af.mil](mailto:afri.aupress@us.af.mil).

# Contents

<b>Disclaimer</b>	<i>ii</i>
<b>List of Illustrations</b>	<i>v</i>
<b>Preface</b>	<i>vii</i>
<b>About the Author</b>	<i>ix</i>
<b>Abstract</b>	<i>xi</i>
<b>1 The Problem</b>	1
<b>2 Context of National Infrastructure Vulnerability</b>	3
Role of ICS and SCADA in Critical National Infrastructure	3
Vulnerabilities	4
Actors	7
Threat Trends	8
Late-to-Need Cybersecurity	11
<b>3 Political Realities</b>	15
Current Challenges to Achieving Effects	15
Precedent Setting and Impact to the Long Game	17
<b>4 National Response Constructs</b>	19
Federal Roles and Responsibilities	19
US Government Response Methodology	24
Cyber Response	26
Noncyber Response	28
<b>5 Recommendations</b>	31
Prevention	31
Detection and Response	36
<b>6 Conclusion</b>	41
<b>Abbreviations</b>	43
<b>Bibliography</b>	45



## List of Illustrations

*Figure*

1	Notional ICS connectivity as potential attack surfaces	5
2	US federal cybersecurity roles and responsibilities	20





## Preface

The research for this paper began with a preconceived notion that the US federal government was woefully behind academia and corporations in assessing and internalizing the risks presented by malicious cyber activity to the nation, especially in the realm of critical national infrastructure. The research led to a completely different conclusion in the end. The White House and executive branch have been, in many cases, leading the call for greater cyber resiliency and cybersecurity across the country. They have been increasingly vocal in this way to defend of our vital national interests. Timing is definitely everything. Although Pres. Barack Obama's administration has been publicly calling for investment, legislation, and coordinated efforts for six years, recent public statements by administration and interagency leadership, and a burgeoning threat landscape in our critical sectors, have galvanized resolve and increased the pace of change.

I would like to take this opportunity to thank my research advisor, Dr. John P. Geis II of the Air Force Research Institute, for his voluminous and exacting feedback over the course of several months. I would also like to thank Mr. Chris Painter, coordinator for cyber issues at the Department of State (S/CCI), Mr. Tom Dukes, and the entire S/CCI team, who have exposed a young Air Force officer to a strategic dialogue and context that wholly informed the tone and fiber in this current discussion. Additionally, I offer my sincere appreciation to Mr. Clayton Romans and Mr. Ben Goldsmith of the Department of Homeland Security; Mr. James Shelton, Department of Defense Computer Network Defense architect; the National Security Agency's Information Assurance Directorate; Col Alan Berry, US Air Force, retired; Mr. Samuel Richardson; and several other key interagency thinkers and policy makers who have helped ground my idealism in reality.



## **About the Author**

Maj Scott A. Weed is the commander, 724th Special Tactics Support Squadron, 724th Special Tactics Group, 24th Special Operations Wing, Pope Field, North Carolina. Major Weed entered the Air Force in 2003 after graduating from the University of Texas at Austin and has served in various assignments in Pacific Air Forces, Air Combat Command, Air Force Space Command, and Air Force Special Operations Command. He has deployed four times to the United States Central Command and United States Southern Command areas of responsibilities, in various leadership roles as flight commander, Task Force J6 (information management), Special Operations Task Force J6 operations officer, and Joint Special Operations Air Component J6.

Major Weed served as the executive officer for the Air Combat Command Directorate of Requirements, the Initiatives Section chief for the Air Force Command and Control Integration Center, the director of operations for the 31st Combat Communications Squadron, and the executive communications support to the commander of United States Force Japan and Fifth Air Force. Before his current assignment, he was an Air Force Strategic Policy Fellow, with duties in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Department of Defense, and in the Office of the Coordinator for Cyber Issues, Office of the Secretary of State, Department of State.



## Abstract

This paper discusses federal efforts to unify the public and private domestic sectors in the defense against cyber attack on the industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that underpin US critical national infrastructure, to offer policy recommendations for synchronizing foreign and domestic cybersecurity efforts, and to realize a resilient and secure infrastructure. The paper intends to provide a policy-level rather than technically-focused discussion. The research was conducted using open-source methods with an intentional focus on US government and media perspectives found in the public record. That is where US international and domestic policies truly take shape.

The discussion begins with an examination of what constitutes critical national infrastructure and the roles of ICS and SCADA systems within it. The paper then describes the panoply of actors, vulnerabilities, late-to-need cybersecurity, and threat trends. The examination also touches on the political and social challenges in achieving greater cybersecurity, and then shifts to a description of how the US government divides efforts among its lead cybersecurity agencies and what responses to a cyber attack on ICS or SCADA might look like. The discussion finishes with recommendations for strengthened international consensus on norms for state behavior, formalized public-private relationships, and interagency efforts to realize a more secure and resilient national infrastructure. Actions on many of these recommendations are under way now in dynamic virtual and policy environments, but their momentum should not diminish or the United States risks ceding its strategic power and security.



## Chapter 1

# The Problem

*Now, the first, the grandest, and most decisive act of judgment which the Statesman and General exercises is rightly to understand in this respect the War in which he engages.*

—Gen Carl Philipp Gottfried von Clausewitz

The new manmade environment of cyberspace is a contested domain, which our critical national infrastructure depends on, which in turn requires greater cooperation for security. As former secretary of defense Chuck Hagel remarked in a September 2014 keynote address, we “are entering an era where American dominance [in] cyberspace—can no longer be taken for granted.”<sup>1</sup> Public and private evidence indicate remarkable upward trends in the cyber threat landscape, especially with observed adversarial and criminal activity throughout our domestic national infrastructure. Actors, motivations, and techniques range widely, yet the potential for significant consequences is undeniable. The president and the interagency community have made great strides in developing guidance and rules of engagement (ROE) to professionalize national activity in cyberspace. However, the true challenge lies beyond a whole-of-government approach and requires energizing the private sector and international community to help achieve a strategically stable and secure global cyberspace construct resilient to malignant activity.

The key aspects of critical national infrastructure issues in cyberspace are the industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems. These systems are key components of infrastructure. ICSs are the interfaces where virtual commands generate physical reality in industrial environments. SCADA systems are the software-based elements of those ICSs. ICS and SCADA systems provide real-time, two-way data flow between sensors, workstations, and other networked devices throughout a system. They allow continuous and distributed monitoring and control. These systems likewise support both human-to-machine and machine-to-machine interfaces with industrial processes, often to promote efficiency and automation.

This paper will discuss the context surrounding critical national infrastructure and the federal efforts to defend ICS and SCADA systems under-

pinning that infrastructure and offer policy recommendations for synchronizing foreign and domestic cybersecurity efforts.

Actors, vulnerabilities, and trends also demonstrate that cybersecurity is behind the curve in many critical sectors. The following chapter outlines the cybersecurity roles and responsibilities across the federal government, recent changes in government processes, and the quest to integrate cyber capabilities into the existing national instruments of power. The following section provides policy and legislation recommendations to improve the resiliency of domestic critical infrastructure and to seek international strategic cyber stability. This paper will not cover the full spectrum of attacks or accidents outside of the cyber domain, nor will it exhaustively detail the landscape of cyber threats. The first concern is to understand properly the environment in which these ICS and SCADA systems operate and how their vulnerability produces risks to our nation.

#### **Notes**

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Hagel, "Defense Innovation Days."



## Chapter 2

### **Context of National Infrastructure Vulnerability**

*Gentlemen, the officer who doesn't know his communications and supply as well as his tactics, is totally useless.*

—Gen George Patton, US Army

The discussion of how the US government might respond to cyber attack on critical infrastructure ultimately rests upon the nation's ability to adapt to complexity and uncertainty. However, we need to understand the technology, risk, and actors at play. The first point of necessary clarification is to understand critical infrastructure as a complex system-of-systems for which policy has only recently formed to articulate its complexity and growing need for cybersecurity. In addition to weaknesses inherent in critical infrastructure due to design, legacy considerations, and environmental dependencies, the realization of burgeoning groups of diverse actors, and worsening threat trends in this space highlight the scale of the problem the US government faces.

#### **Role of ICS and SCADA in Critical National Infrastructure**

This paper uses the presidential definition of critical national infrastructure detailed in Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of [such] would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>1</sup> Because of this, mounting cyber threats to critical infrastructure represent “one of the most serious national security challenges we must confront.”<sup>2</sup> Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, refines this concept by detailing the 16 foundational critical sectors as:

- chemicals,
- commercial facilities,
- communications,
- critical manufacturing,
- defense industrial base,

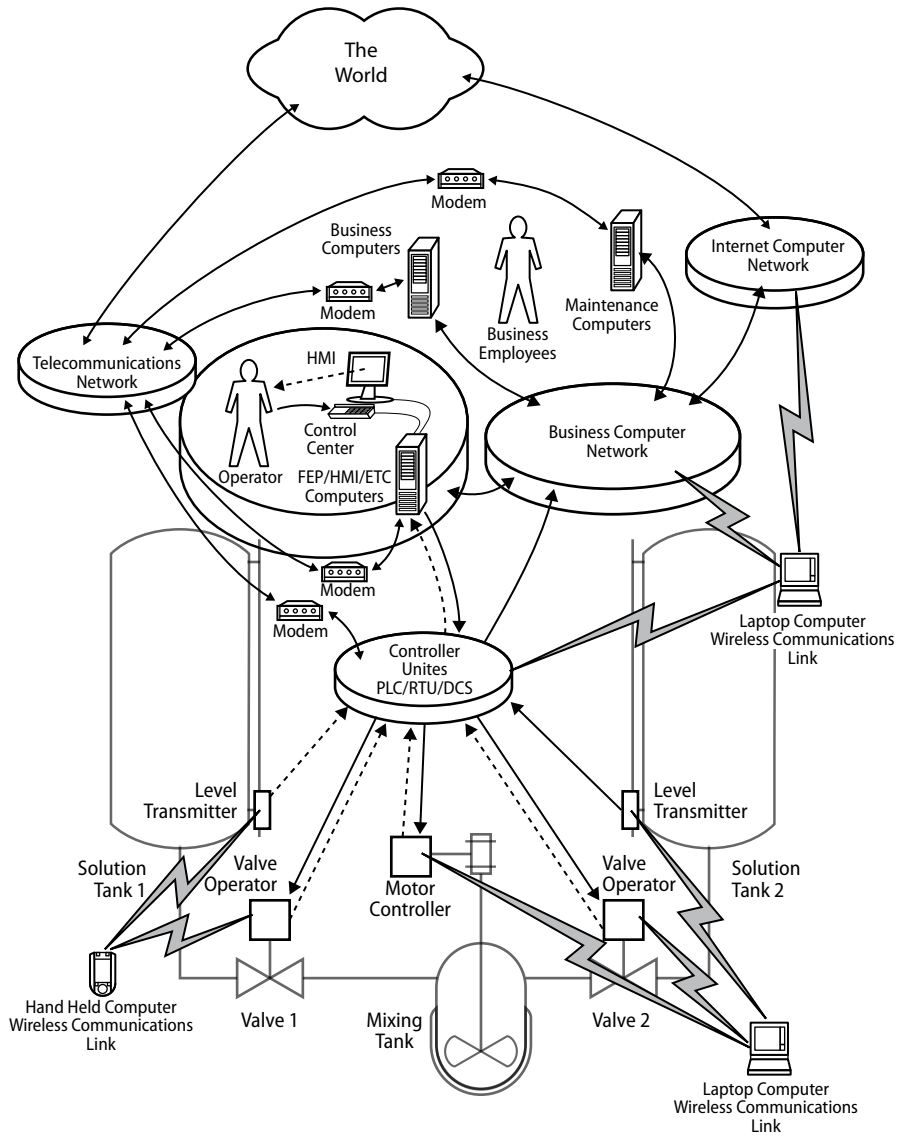
- dams,
- emergency services,
- energy,
- financial services,
- food/agriculture,
- government facilities,
- public health,
- information technology (IT),
- nuclear,
- transportation, and
- water/wastewater.<sup>3</sup>

For the purposes of this paper, critical infrastructure will consist of these 16 PPD-identified sectors.

According to PPD-21, critical infrastructure depends on complex “distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multilevel authorities, responsibilities, and regulations.”<sup>4</sup> The directive specifically identifies “energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.”<sup>5</sup>

## **Vulnerabilities**

The primary causes of ICS and SCADA vulnerabilities fall into three general categories: insecure design, the human element, and configuration issues, all of which are either implicitly or explicitly articulated in figure 1. An insecure design approach failed to take into account the contested, interdependent, and complex environment in which these systems would operate. Also, the presence or absence of human control and influence can also be a cause for certain systemic vulnerabilities. Finally, poorly or negligently configured equipment provide opportunities for attackers to compromise systems that otherwise would have been secure. Investigators discovered a combination of these factors at play in 2003 when a chance encounter between a power line and a tree touched off a rippling chain of events that led to the simultaneous failure of two interconnected units and culminated in the largest blackout in North American history.<sup>6</sup>



**Figure 1. Notional ICS connectivity as potential attack surfaces.** (Reproduced from Industrial Control Systems Cyber Emergency Response Team website, n.d. <https://ics-cert.us-cert.gov>, accessed 19 October 2014.)

The first major source of SCADA vulnerability lies in an insecure design approach. PPD-21 emphasizes the complexity of the security challenge in

noting that “just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities.”<sup>7</sup> Therefore, a design approach that infuses cross-domain considerations with security is required throughout. SCADA, as highlighted in figure 1, often overly depend on disparate and heterogeneous communications protocols, topologies, and links between controller units, sensors, human-machine interface subsystems, databases, engineering workstations, mission control centers, and business office networks. Each of these, if not designed securely, represent potential footholds or jumping-off points for malicious actors.<sup>8</sup> The patchwork composition for many ICS and SCADA systems present a diverse architecture that can become intractable to forensic analysis and defense.

The human element is ubiquitous across all ICSs and can represent great strengths or vulnerabilities depending on human capability and intent. Increased automation of SCADA systems endeavors to increase machine-to-machine interfaces and reduce costs.<sup>9</sup> However, humans are common in most infrastructure environments whether visiting, monitoring, troubleshooting, maintaining, or controlling those systems. These individuals can then be manipulated through spear phishing, social engineering, or direct elicitation.

The next area of concern is poor configuration of services and devices. This is the most common vulnerability yet the easiest and most economical to control. Organizations are starting to observe configuration vulnerabilities in the operational technology supporting their critical processes, previously only seen in traditional IT networks. There is also a tendency to employ lower-cost, commercial-off-the-shelf technologies in critical operating environments. This represents huge risk when technologies are not properly hardened during configuration and left to run in settings discoverable on the open Internet. In general, weakly-enforced technical and administrative internal security measures have led to critical systems being directly connected to the external Internet for convenience, making them much easier targets for compromise.

One initiative to bring attention to cybersecurity in the SCADA community was Project SHINE, a two-year-long search and assessment of the publicly available information on ICS and SCADA systems connected directly to the Internet. Project SHINE utilized a custom search engine to perform the first large-scale data mining of cyber intelligence for such systems. It frequently yielded “the IP [Internet protocol] address of the device, geographic location (including latitude and longitude coordinates), owner, service port header information, firmware details, and available protocols.”<sup>10</sup> The detail and scale of the results were astounding, as the search discovered 2.2 million distinct devices, many of which system operators would have never previ-

ously conceived of as vulnerable entry points. “HVAC [heating-ventilation-air-conditioning] and automation systems [were] important considering many attackers are using these systems as an indirect avenue of attack, [which] let attackers come into the network and scan to find out what other systems are accessible.”<sup>11</sup> The overall assessment of Project SHINE was that, either through ignorance or negligence, most organizations simply do not understand how their systems interact with the outside world and the risks that follow.<sup>12</sup> Whether misconfiguration or systemic vulnerabilities introduce the risk, the resulting impact to the ICS may be indistinguishable from adversarial activity and still yield consequences for production, revenues, and safety.

Indications are that potential adversaries, terrorists, and other malicious actors may not need to generate the total failure of a massive hydroelectric dam or transportation system but could achieve the same effect through a targeted cyber operation designed to induce cascading systemic failure from an isolated pipeline or generator exploitation. An understanding of ICS and SCADA vulnerability, however, is incomplete without a discussion of the adversary.

## **Actors**

The actors at the heart of this discussion vary in nature, from peer and non-peer nation states to nonstate actors such as terrorists, criminals, insiders, patriotic hackers, malware writers, botnet herders, and other illicit entrepreneurs.<sup>13</sup> The threat posed by each of these subpopulations is real, and any combination of them is more than the sum of its parts. Nonstate actors ensure that governments do not own a monopoly on violence in cyberspace. With lowering barriers to entry, cyber capabilities proliferate as rapidly as “software can be copied more easily than a tank or a rifle.”<sup>14</sup> Terrorists, such as al-Qaeda, have called for “electronic jihad” against American critical infrastructure.<sup>15</sup> Also, if a sponsor has funds but lacks access or skills, they may elect to hire cyber mercenaries as effective proxies. Motivations range from national economic or military advantage to sabotage, theft of intellectual property, deception for a subsequent attack, nationalistic fervor, influence operations, and even outright nihilism. Unlike the other domains that afford physical demarcation to divide the global commons into sovereign elements, in cyberspace, both friends and adversaries traverse, operate in, and depend on upon the same network, often with commerce or recreational traffic commingling with activities of national security importance.<sup>16</sup>

Intentional cyber exploitations or attacks come in phases. Often they ultimately target data or service reliability to undermine the “welfare and secu-

rity of individuals, businesses, nations, and the globally-linked international community as a whole.”<sup>17</sup> Attacks that target SCADA must first gain access to the control system, elevate privileges, enumerate or map the virtual environment, move laterally across systems, comprehend processes at work, and then exploit a process.<sup>18</sup> An exploited SCADA system can be used in “issuing unauthorized commands to control equipment; sending false information to a control-system operator that initiates inappropriate action[;] delaying or blocking the flow of information[;] making unauthorized changes to control system software to modify alarm thresholds or other configurations; and rendering resources unavailable.”<sup>19</sup>

## Threat Trends

*Malicious actors exploit networks no matter where they are located.*

—United Nations Groups of Governmental Experts

The cyber threat facing our nation has risen to unprecedented levels of attention in policy-making circles. Director of National Intelligence James Clapper testified before the Senate Armed Services Committee in February 2015 that cyber attacks against both US government and civilian networks represented the most serious worldwide threat to the United States.<sup>20</sup> Maj Gen John A. Davis, US Army, the senior military advisor to the deputy assistant secretary of defense for cyber, echoed the trend succinctly when he stated “the level of risk that cyber adversaries pose to our country’s economic and national security has become more sophisticated, more pervasive, and more threatening.”<sup>21</sup> More alarming is the assertion from Rep. Mike Rogers (R-AL), chairman of the House Intelligence Committee, that while the private sector represents 85 percent of US networks, they are not ready to respond or adapt to “even present-day hacks from nation-states, much less a coordinated retaliatory back and forth of extremely sophisticated attacks . . . that might be characterized as cyber war.”<sup>22</sup>

Defense of ICS and SCADA systems is a critical subset of the overall national cybersecurity challenge, and there are many methods adversaries can utilize to attack such systems. ICS and SCADA threats, as articulated in PPD-21, fundamentally require an “all-hazards” perspective, encompassing more than just cyber threats.<sup>23</sup> This holistic approach targets the relationships and dependencies that present systemic vulnerability. For example, there is the susceptibility of SCADA systems to solar flare radiation or the catastrophic failure of nuclear reactors due to a tsunami.<sup>24</sup> While these other threats are

important, as stated in the introduction, this paper will focus exclusively on the cyber threats, whether from states, groups, or individual actors.

The opportunities for a cyber attack on SCADAs are replete with various methods and avenues of attack to achieve devastating effects on a target network. The effects of data manipulation, instrument alteration, or power fluctuation upon an ICS or SCADA systems represent scenarios where cyber generates tangible effect upon businesses or governments. Points of attack may include an ICS, external office IT network, calibration tools, field devices, safety systems, technician support equipment,<sup>25</sup> and even the employees themselves. Any avenue designed to provide convenience or greater capability to an authorized user typically has benefits for an attacker. Take the consolidation of ICS and safety systems into a single, integrated control and safety system. This presents a single, consolidated target. Threats may also include supply-chain targeting of firmware and devices—hidden cameras, keyboards, cables, and peripherals; malware capable of jumping gaps between IT, ICS, and other air-gapped networks—ICS process-focused effects; and general alteration of data or depletion of resources.<sup>26</sup>

The national leadership attention provided to this problem set is directly proportional to the increased public reporting of compromises by both state and nonstate actors. There have been a startling number of reports recently, including a coordinated cyber intrusion into US pipeline SCADA systems, Russian hackers exploiting Western energy companies and ICSs in 23 countries, Chinese and Russian mapping of the US electrical grid, regional conflicts such as the Syrian civil war bleeding into cyberspace, and unknown hackers shutting down an oil platform by inducing unsafe tilting.<sup>27</sup> There is also growing speculation North Korea could capitalize on known vulnerabilities, and indications that Iranian actors “have directly attacked, established persistence in, and extracted highly sensitive materials from [major] critical infrastructure companies.”<sup>28</sup>

Also, several recent and public cyber attacks on ICSs or SCADAs have generated catastrophic results. The first publicly released and highly formative demonstration of ICS vulnerability was the Aurora Generator Test conducted by the Idaho National Laboratory in 2007, where the intentional and rapid opening and closing of breakers in a commercially available generator induced an out-of-phase condition that effectively destroyed the equipment when connected to the power grid.<sup>29</sup> Security experts extrapolate that the Aurora vulnerability is not merely constrained to generators but extends to electrical systems and rotating equipment elsewhere, such as in manufacturing, refineries, data centers, and mass transit.<sup>30</sup> In San Bruno, California, in 2010,

a SCADA failure and mechanical compromise resulted in a pipeline explosion that “killed eight people, injured 60 others, and destroyed 37 homes.”<sup>31</sup>

A recent and corroborated example of cyber being utilized to target infrastructure was the cyber attack on a German steel factory detailed in a late 2014 IT security report. Attackers used a combination of traditional exploitation techniques (e.g., spear phishing and social engineering) to gain access to office networks and, in turn, the production ICS network, which led to a spike in equipment failures across the plant and ultimately in significant damage to the blast furnace, rendering the plant inoperable.<sup>32</sup>

Evasive and evolving advanced cyber tools like Stuxnet, Regin, and Flame represent the current benchmark for modern offensive cyber capability. Stuxnet spread indiscriminately in the wild, ultimately leading to its discovery. Yet the payload only affected highly specific Siemens SCADA systems tied to covert Iranian nuclear centrifuges. The Stuxnet payload surreptitiously altered performance data to the detriment of the enrichment process. Security experts now suggest that Stuxnet no longer represents the cutting-edge of offensive cyber tools, as security researchers observe and analyze far more advanced cyber tools such as Regin, Flame, and other yet-to-be-named capabilities that are only just now observable and subject to analysis.<sup>33</sup>

It is important to note that beyond the purview of this paper, advanced adversaries would likely utilize hybrid asymmetric attacks to achieve greater effects by combining cyber operations with information operations, unconventional warfare, or economic sabotage. A documented instance of such attacks was the 2013 well-coordinated physical attack on a Pacific Gas and Electric substation, where unknown attackers intentionally severed six fiber-optic lines and fired over 100 rounds of ammunition into transformers. This represented a “game changer” for those charged with critical infrastructure physical security.<sup>34</sup>

In unprecedented official recognition of the threat to SCADA, Adm Michael Rogers, US Navy, director of the National Security Agency (NSA) and commander of US Cyber Command (USCYBERCOM), testified before Congress that “China and ‘one or two’ other countries are capable of mounting cyber attacks that would shut down the [US] electric grid and other critical systems.”<sup>35</sup> Any uncertainty in whether the United States appreciates the gravity of this problem set is eliminated in the clearest terms of EO 13636, as “it is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure.”<sup>36</sup>



## Late-to-Need Cybersecurity

SCADA systems too frequently carry an insufficient level of cybersecurity for the importance of the systems they support. This is mainly due to historically insular and permissive principles of system design or misapplied traditional IT practices, which have proven inadequate in a modern cloud-based, distributed, interoperable, and interconnected environment. Current IT networks have shifted away from the defense-in-depth model that had come to dominate corporate and government network design. This is because of an overreliance on the artificial “inside” versus “outside” modality that cannot deliver mission assurance in a contested cyber world. Also, SCADA systems are often not updated to deal with evolving and multiplying malware; they rely on legacy protocols foreign to modern firewalls; they lack identity management; and they avoid controls and monitoring “commensurate of the mission criticality of the systems.”<sup>37</sup> Antiquated and static IT security practices designed for a permissive environment cannot effectively defend these architectures, especially when advanced nation-state actors have been observed actively developing capabilities to target SCADA systems.<sup>38</sup>

Critical infrastructure owners are “uniquely positioned to manage risk [and] determine effective strategies.”<sup>39</sup> However without catalytic events or appropriately strong regulatory regimes, these owners gravitate towards profit considerations rather than significantly more certain continuity of operations and greater national good to be realized through cybersecurity, testing, and resilience.<sup>40</sup> Overall, national standards and regulation compliance remain largely voluntary in industries that have yet to experience a catastrophic event. An exception is the domestic electric sector and its adherence to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards.<sup>41</sup> A sustained Iranian distributed denial-of-service (DDOS) campaign in 2012–2013 against the US financial industry did generate a notable sector response, evident when J. P. Morgan decided to double its cybersecurity investment profile, yet these kinds of response remain exceedingly rare instances.<sup>42</sup> Faced with low corporate and congressional appetite for regulation, the executive branch must advocate that critical infrastructure cybersecurity is a matter of both national security and corporate survival.

Cybersecurity for SCADA systems is no longer restricted to federal or large organizations, as regional and local entities are increasingly targeted with specifically engineered attacks. Nation-states are beginning to target state, local, tribal, and territorial (SLTT) networks in cyberspace. Historically this was only anticipated for federal networks. Any presumed sanctuary of scale or obscurity was thereby shattered. Compared to hardened federal systems,

SLTT or corporate entities may provide a path of least resistance to attack. In the early 2000s, most ICS attacks were incidental and believed to be collateral or unintended damage from broader, conventional IT incidents. Yet, in 2010, security researchers began to observe customized tools and techniques that indicated understanding and intent to target ICS and SCADA systems.<sup>43</sup>

#### Notes

1. Executive Order (EO) 13636, Improving Critical Infrastructure.
2. Ibid.
3. Presidential Policy Directive (PPD) 21: Critical Infrastructure.
4. Ibid.
5. Ibid.
6. Minkel, “2003 Northeast Blackout.”
7. PPD 21: Critical Infrastructure.
8. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) website.
9. Parfomak, “Pipeline Cybersecurity.”
10. Rashid, “Project SHINE Reveals Magnitude.”
11. Ibid.
12. Ibid.
13. Martin and Kirschbaum, “Pro-Russian Group Claims Cyber Attack.”
14. Geers, “Cyberspace and the Changing Nature of Warfare.”
15. Cloherty, “Virtual Terrorism.”
16. Ibid.
17. Department of Defense (DOD), “United States Government Submission.”
18. ICS-CERT website.
19. Parfomak, “Pipeline Cybersecurity.”
20. Taylor, “James Clapper.”
21. Davis, Keynote Address.
22. Tucker, “House Intel Chief Wants to Increase Cyber Attacks.”
23. PPD 21: Critical Infrastructure. The “all-hazards” threats to critical infrastructure posed by PPD-21 include “natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity.”
24. ICS-CERT, ICS-CERT Advisory;” and World Nuclear Association. “Fukushima Accident.”
25. Assante, “ICS/SCADA Security Challenges and Developments.”
26. Ibid.
27. Parfomak, “Pipeline Cybersecurity”; Perloth, “New Security Report Confirms”; Perloth, “Russian Hackers Targeting”; Gorman, “Electricity Grid in US”; and Wagstaff, “All at Sea.”
28. Tucker, “Forget the Sony Hack”; and Cylance, “Operation Cleaver Report.”
29. Swearingen et al., “What You Need to Know.”
30. Ibid.
31. Parfomak, “Pipeline Cybersecurity.” The 30-inch diameter natural gas pipeline exploded due to an attack that left the SCADA unable to respond to overpressure indications.
32. Kovacs, “Cyberattack on German Steel Plant.”
33. Zetter, “An Unprecedented Look at Stuxnet”; and Kaspersky Lab, “Regin Platform.”

34. Reilly, "Bracing for a Big Power Grid Attack."
35. Dilanian, "NSA Director."
36. EO 13636, Improving Critical Infrastructure.
37. James Shelton, computer network defense architect for the DOD chief information officer, interview by the author, 2 February 2015.
38. Assante, "ICS/SCADA Security Challenges."
39. PPD 21: Critical Infrastructure.
40. Geis, et al., *Blue Horizons IV*, 13.
41. North American Electric Reliability Corporation, *Critical Infrastructure Protection (CIP) Standards*.
42. Nakashima, "Iran Blamed for Cyberattacks"; and Glazer, "J. P. Morgan CEO."
43. Ibid.



## Chapter 3

### **Political Realities**

The US government must first appreciate social realities, corporate motivations, and political precedents before fully developing policy responses to cyber attack on critical infrastructure. The president outlined the national approach to this problem in PPD-21, which asserts that the United States will strengthen critical systems against emerging threats by working across public and private sectors while emphasizing the role of private owners and operators in securing their systems.<sup>1</sup> General Davis reinforced the criticality of this partnership with the private sector when he highlighted that “over 99 percent of the electricity and 90 percent of the voice and communications services that the military relies on comes from civilian sources.”<sup>2</sup> The federal government cannot achieve success in this fight without nongovernmental support.

### **Current Challenges to Achieving Effects**

Recurring challenges hinder translation of thoughtful and measured federal response policies into reality. This is due in no small part to the perceived immaturity of cyberspace, the patchwork of stakeholders, and conflicting public and private interests. The incipiency of cyberspace and the difficulty of calculating and delivering cyber effects generates concern that errant cyber activity might degrade or disrupt international and dual-use cyberspace and generate negative strategic effects. Varying degrees of cultural dissonance across the various defense, intelligence, law enforcement, diplomatic, and private sector communities responsible for critical infrastructure protection also exists. Each operates with its perspectives, biases, and sets of objectives. These aspects emphasize the need for transparent and well-coordinated policy, inclusive of private stakeholders and rooted in information sharing at all levels.<sup>3</sup>

The US government strives for a balance between protecting the civil liberties and freedoms rooted in our founding principles with the need for greater security—expanded surveillance and information sharing at home and abroad. PPD-20, United States Cyber Operations Policy “provides a whole-of-government approach consistent with the values we promote both domestically and internationally.”<sup>4</sup> General Davis reaffirms this by asserting the US government will only act when network defense or law enforcement activities

fall short, using the least force required, and will only do so in accordance with the US Constitution, laws, and policies.<sup>5</sup> Section Five of EO 13636 specifically requires the Department of Homeland Security (DHS) to reevaluate continually risks to private and civil liberties, resulting from any cybersecurity initiatives.<sup>6</sup> EO 13636 also pushes federal agencies to increase reporting, prioritize corporate security clearances, and encourage cross-flow of industry experts into government positions—all with the express intent of increasing transparency and preserving civil liberties.<sup>7</sup>

A significant challenge to achieving a whole-of-nation cybersecurity mindset is the reluctance among corporate executives to place security ahead of business needs and profits. As retired Air Force General Michael Hayden, former director of the NSA and of the Central Intelligence Agency, observed, “The free market has failed to provide an adequate level of security for the Net.”<sup>8</sup> Traditional business risk frameworks do not universally adapt to dynamic and persistent cyber threats without concerted corporate effort and may thus fail to convince the C-suite (senior management) that cyber vulnerability ultimately undermines business goals. Even among the subset of critical infrastructure facilities the federal government regulates, system owners have yet to formalize cyber aspects into their emergency action plans, continuity of operations, or resilience planning. SCADA cybersecurity must not only be understood as valuable to the greater business in a profit-driven environment—not unlike insurance costs to mitigate risk—but it must also be appreciated as foundational to the national greater good. There is, of course, the reality of increasing threats and ever-constrained resources that public and private leaders will continue to balance.

The exponential growth of cyber threats and diminishing federal budgets are forcing policy makers to abandon the goal of complete protection and, rather, implement risk mitigation and mission resilience measures for asset protection. Capitalizing on cross-sector, real-time, actionable threat intelligence and shifting from a static defense-in-depth strategy to a dynamic framework that focuses on adversaries is the only way to ensure a maximum return on limited security resources. In the longer term, a greater emphasis on cybersecurity-focused system design and acquisition for new systems is vital. Admiral Rogers asserted that systems must evolve “to sustain damage and still achieve mission outcomes,”<sup>9</sup> and the same holds in ICS and SCADA environments. Finally, US domestic and foreign policy directly underpin response options to cyber attack, and policy makers must examine these options against the international and political situation.

## Precedent Setting and Impact to the Long Game

The United Nations Group of Governmental Experts (UNGGE) in June 2013 made a landmark determination that international laws, including the UN Charter, extend into and apply in cyberspace.<sup>10</sup> The UNGGE also recommended states work with academic and corporate stakeholders to promote an open, stable, and secure cyberspace. This would ideally be done with the adoption and application of norms of conduct and other “voluntary measures to increase transparency, confidence, and trust among States.”<sup>11</sup> This recommendation relies on existing international frameworks and time-tested legal precedent. The UNGGE recommendation is analogous to the development of international maritime law, precluding the creation of new ad hoc systems. The United States is resolute in its support of the UNGGE recommendations.<sup>12</sup>

The 2014 North Atlantic Treaty Organization (NATO) Wales Summit further affirmed the UNGGE recommendations by maintaining that “international law, including international humanitarian law and the UN Charter, applies in cyberspace.” NATO’s assertion is categorical—cyberspace will not be a lawless space. NATO also determined that cyber attacks could threaten national security and stability, holding that “cyber defence is part of NATO’s core task of collective defence” meriting case-by-case Article 5 consideration.<sup>13</sup> It is worth noting that neither the UN nor NATO yet specifies a specific “red line” response threshold, automatically determining retaliation and strategic options. Without established and recognized norms of cyber behavior to frame the use of national instruments of power, “We could be forced to live in the worst of all possible cyber worlds—routinely vulnerable to attack and self-restrained from bringing our own power to bear.”<sup>14</sup>

There is also significant policy context necessary for any US cyber response. The US *International Strategy for Cyberspace* holds that existing Internet governance bodies should continue to guide and shape the development of the Internet.<sup>15</sup> The US strategy is aimed at continuing the Internet tradition of innovation, rather than a competing vision of state control. The United States desires to ensure appropriate representation from governments, academia, and private and civil sectors.<sup>16</sup> US policy makers insist on not conflating control over standards and protocols with a perceived (by some) need for sovereign ability to act unilaterally or multilaterally in cyberspace to preserve vital national interests.

Policy makers and strategists must likewise endeavor to stay informed by and ahead of technology. In this way, there must be consensus about distinguishing among sophisticated cybercrime, ubiquitous cyber espionage, and

legitimate cyberwarfare. The current blurred lines among these three are often used by adversaries in cyberspace to disguise and obscure intent and patronage.<sup>17</sup> States should also realize that policy decisions in cyberspace will likely have international consequences due to interconnectedness, and there should be understood requirements for “global interoperability, network stability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.”<sup>18</sup> This well-informed spirit of transparency in policy would help mitigate the fog of war inherent in cyber incidents and potentially avert unnecessary conflict.<sup>19</sup> The political landscape and societal contexts are not the only considerations. There is also the development of the US whole-of-government approach to respond to cyber attack.

#### Notes

1. PPD 21: Critical Infrastructure.
2. Davis, Keynote Address.
3. Assante, “ICS/SCADA Security Challenges.”
4. Davis, Keynote Address.
5. Ibid.
6. EO 13636, Improving Critical Infrastructure Cybersecurity.
7. Ibid.; and PPD 21: Critical Infrastructure.
8. Hayden, “Future of Things ‘Cyber.’”
9. Boyd, “IT Security Shifts.”
10. United Nations Group of Governmental Experts (UNGGE), “Developments in the Field.”
11. Ibid.
12. Davis, Keynote Address.
13. NATO, “Wales Summit Declaration.” Article 5 of the North Atlantic Treaty deals with the requirements of collective defense of alliance members.
14. Tucker, “Forget the Sony Hack”; and Hayden, “Future of Things ‘Cyber.’”
15. White House, *International Strategy for Cyberspace*.
16. Daniel, Holleyman, and Niejelow, “China’s Undermining an Open Internet.”
17. Hayden, “Future of Things ‘Cyber.’”
18. Mary Beth Morgan, director, Cyber International Strategy, Office of the Secretary of Defense, discussion with the author, 17 October 2014.
19. DOD, “United States Government Submission.”



## Chapter 4

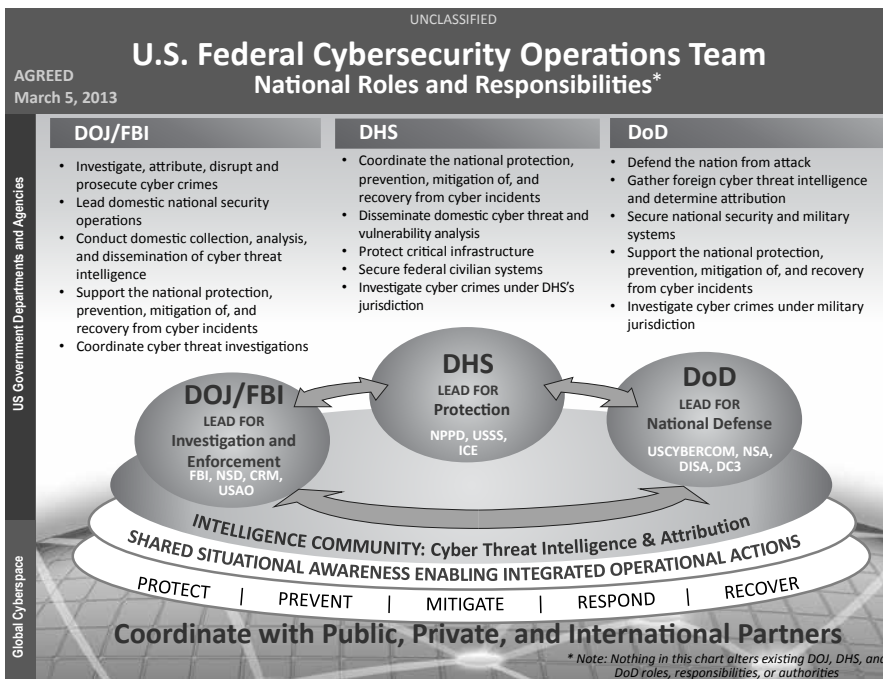
### **National Response Constructs**

The US government has made significant efforts to unify a historically piecemeal federal approach to cybersecurity, especially in response to the threats to our critical national infrastructure—an essential and vulnerable center of gravity of our American way of life. Fortunately, and unlike the after-the-fact reforms of the Goldwater-Nichols Act, the federal government is moving proactively to bring about procedural and cultural changes before there is a major loss. This whole-of-government approach provides unprecedented clarity and unity of effort through concise policy, interagency deconfliction, and standing ROEs. All these measures are to be continually refined through exercises and further dialogue across public and private sectors. The capabilities to detect, blunt, and respond to a cyber attack on ICS or SCADA systems directly defends business continuity, public safety, and US national interests.

### **Federal Roles and Responsibilities**

The US government only recently formalized the federal cyber interagency process in a much-needed effort to coordinate the vast array of governmental organizations and voices. The Principals Committee, Deputies Committee, and interagency policy committees provide White House-led coordination mechanisms bridging the National Security Staff with federal departments and agencies through routine meetings, tasks, and deliverables. The White House additionally recognized the need to bring all of the federal stakeholders into a single forum to achieve an effective cyber incident response; so, the administration stood up the Cyber Response Group (CRG) in 2014, modeled after a similar successful approach to counterterrorism after 11 September 2001.<sup>1</sup> The CRG unifies elements of the administrative, defense, law enforcement, intelligence, homeland security, diplomacy, and myriad of other functions to ensure a whole-of-government approach that can adapt and respond to rapidly emerging and ambiguous cyber threats.

Figure 2 represents the first codified interagency consensus on a division of labor across the three primary federal cybersecurity agencies. However, the roles and responsibilities remain anchored to incident response without explicit roles for foreign engagement, economic policy, or other federal activities. This single diagram does represent a landmark interagency agreement as it required over 60 coordinated iterations before being finalized.<sup>2</sup>



**Figure 2. US federal cybersecurity roles and responsibilities.** (Reproduced from Industrial Control Systems Cyber Emergency Response Team website, n.d. <https://ics-cert.us-cert.gov>, accessed October 19, 2014.)

The Department of Justice (DOJ)—specifically the Federal Bureau of Investigation (FBI)—enforces the rule of law and accountability, where possible, using various investigative and legal tools.<sup>3</sup> DOJ efforts to investigate and discern forensic trails provide law enforcement options in conjunction with other instruments of national power. The FBI continues to operate the “National Cyber Investigative Joint Task Force (NCIJTF), [serving] as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, IC [intelligence community], DOD [Department of Defense], and other agencies as appropriate.”<sup>4</sup> Also, the FBI provides rapid cyber incident notification for the situational awareness of all participating private organizations through the FBI Liaison Alert System (FLASH) and voluntary InfraGard initiative. Finally, the FBI synchronizes threat information from multiple partnering agencies, using its in-house Cyber Guardian cross-domain database, to ensure efficient victim notification and mitigation development.

The DOD, with USCYBERCOM as its principle agent, conducts full-spectrum military operations in and through cyberspace to protect the homeland, enable operations in other war-fighting domains, and provide freedom of action for the United States and its allies. Military cyber operations typically focus on defensive and offensive capabilities in support of larger operational or strategic objectives. However, intelligence gained in defending and maintaining one of the largest and most targeted worldwide networks can often provide critical information on possible threats and attacks against the ICS and SCADA sectors.<sup>5</sup> Specialized teams within USCYBERCOM forces, when appropriately tasked, have the ability to deploy either virtually or physically to domestic facilities to augment other federal agencies in the protection of critical national infrastructure. Mechanisms to maintain discretion are critical because either federal law enforcement or military deployment into private installations could have damaging consequences for shareholder and market confidence. Finally, DOD cyber and traditional military capabilities ultimately underwrite US deterrence and response.

The DHS, with the National Protection and Programs Directorate (NPPD), leads the federal charge to secure national cyber and physical infrastructure.<sup>6</sup> According to PPD-21, DHS “shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation’s critical infrastructure.”<sup>7</sup> NPPD not only protects federal government networks but also coordinates and executes protection efforts for critical infrastructure systems against physical and cyber threats through private-sector partnerships.<sup>8</sup> Additionally, NPPD can respond and augment organizations experiencing cyber incidents when requested to assess and recommend mitigation strategies.

DHS and NPPD operate the National Cybersecurity and Communications Integration Center (NCCIC), which serves as the focal point for overall cybersecurity and communications protection across public and private sectors. The NCCIC operates under the National Cyber Incident Response Plan (NCIRP) that governs responses to significant cyber incidents. This is how network defense, law enforcement, intelligence, defense, and civilian communities safeguard critical national infrastructure.<sup>9</sup>

The NCCIC has four main branches, two of which apply here: the US Cyber Emergency Response Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The US-CERT is responsible for defending US networks in general, using tools like the National Cybersecurity Protection System (also known as “Einstein”) program featuring signature-based sensors to detect malicious Internet traffic and forming the basis of federal detection and initial cyber response capabilities.<sup>10</sup> The

ICS-CERT focuses on ICS/SCADA system cybersecurity through robust public-private partnerships, since most of these systems are nongovernmental. ICS-CERT emphasizes four main lines of effort: situational awareness, vulnerability coordination, incident response, and strengthening public-private cybersecurity partnerships.

ICS-CERT utilizes professional relationships, coordinating bodies, and its expert role to pursue its mission. Like US-CERT, ICS-CERT also strives to develop relationships with foreign cyber emergency response teams to improve international cyber hygiene by sharing security incident information, mitigation measures, and best practices,<sup>11</sup> in addition to building partnership capacity. ICS-CERT oversees the “Critical Infrastructure Cyber Community Voluntary Program [(C3VP) as] the coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber risk management processes.”<sup>12</sup> Using the Industrial Control Systems Joint Working Group (ICSJWG), ICS-CERT exercises cross-sector leadership, driving the collaborative design and development of secure ICSs. ICS-CERT’s Idaho National Laboratories offer invaluable virtual, instructor, and hands-on training opportunities in ICS cybersecurity.

The NCCIC serves as a trusted industry partner as a critical infrastructure protection program. It affords unique protection for cybersecurity disclosures from Freedom of Information Act requests, civil and criminal discovery actions, and trade-secret waiver.<sup>13</sup> The current Cyber Information Sharing and Collaboration Program (CISCP) and Enhanced Cybersecurity Services (ECS) programs are prime examples of DHS-led trust-based cybersecurity information-sharing environments between federal, SLTT, and private entities. These programs also emphasize protection of privacy and civil rights. ECS, for instance, provides unique conduits to share classified and sensitive cyber threat intelligence with either service providers or network defenders, all based on an established voluntary and formal vetting relationship between DHS and other participants.

New cyber collaboration tools also exist that facilitate trusted and automated information sharing between the NCCIC and network defense community, like the Structured Threat Information eXpression (STIX™) and the Trusted Automated eXchange of Indicator Information (TAXII™). STIX™ establishes a data standard that allows automated threat interpretation in for active cyber defense. TAXII™ outlines a standard interface of secure services and exchanges intended to streamline automated information flow between organizations. Although DHS orchestrates these efforts, the tools remain highly informed and influenced by international governance and standards organizations.

Information sharing and analysis centers (ISAC) are not official elements of the federal government, yet they are central to the US government strategy and DHS's ability to manage and protect critical infrastructure and key resources (CI/KR), particularly since most of these systems reside in the private sector. CI/KR operators trust and empower ISACs to coordinate, speak, and act in the interest of a given sector and to engage with the federal government and with other sectors. ISACs emphasize an "all-hazards" approach to protecting these systems. They also often provide members a full-time security operations center (SOC), threat information sharing, and anonymous reporting mechanisms.<sup>14</sup> The success of ISACs as collaborative cyber and physical security enclaves has led to their adoption in subsequent information-sharing constructs.

DHS additionally developed the National Institute for Cybersecurity Education (NICE) as a broad initiative to align and standardize cybersecurity knowledge, skills, and tasks across academia, industry, and policy makers. NICE, in turn, has produced the National Cybersecurity Workforce Framework designed to overhaul and reform the antiquated federal cyber career management system, which had previously inappropriately grouped disparate skill sets into amalgamated labor pools. This new framework will allow accurate and granular accounting of cyber expertise. This, in turn, will improve the federal management of these critical fields and allow more robust and deliberate individual development. The Office of Personnel Management will eventually translate this new framework into standard federal practice.<sup>15</sup>

DOJ, DOD, and DHS efforts provide an incomplete picture of the US government's responses to cyber threats. There are many other federal government roles in the protection of cyberspace. The Department of State (DOS) is the national foreign policy arm. DOS uses diplomatic channels, like the UN, to further the international dialogue on cyber behavior norms and the need for a cooperative approach to developing a stable and secure cyberspace. Diplomacy is also used to request assistance from other nations regarding cross-border cyber activity. DOS is the lead agency in international consensus-building and decision-making where diplomacy represents the primary US lever of power.

The Director of National Intelligence (DNI) and the IC serve as the repository and disseminator of critical intelligence for early warning and threat indicators to government, industry, and academia, while deconflicting IC cyber operations. The DNI will also oversee the newly designated Cyber Threat Intelligence Integration Center, which will serve as the federal government hub of threat assessment, all-source integration, and intelligence sharing, to empower federal cyber centers, operators, and policy makers.<sup>16</sup>

The Department of the Treasury provides unique investigative capability to “follow the money.” It also enforces sanctions against “bad” actors, such as in the case of the 2014 Sony cyber attack that was successfully attributed to North Korea.<sup>17</sup> The Office of Management and Budget helps translate administrative guidance into action, provides regulation oversight, and adjudicates appeals for critical infrastructure designation under EO 13636. In late 2014 a dedicated unit intended to engage the interagency staff in strengthening federal cybersecurity was also created.

The Department of Commerce’s National Institute of Standards and Technology (NIST) is the preeminent organization for setting standards and promoting security related to critical national infrastructure in the United States.<sup>18</sup> EO 13636 specifically directed NIST to provide a Cybersecurity Framework “to reduce cyber risks to critical infrastructure” through “a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches.”<sup>19</sup> This Cybersecurity Framework, released in February 2014, specifically recognized that private sector buy-in and adoption was crucial to the success of the effort, and was thus a product heavily influenced and shaped by joint government-industry interaction.<sup>20</sup>

The Department of Energy (DOE) operates the National SCADA Test Bed Program, which focuses on security challenges to the energy-sector ICS.<sup>21</sup> The various national laboratories pioneer cutting-edge ICS and SCADA cybersecurity solutions, such as quantum cryptographic key distribution, automated risk analytics, dynamically shifting defenses, anomaly detection, and critical supply-chain validation.<sup>22</sup> PPD-21 and the National Infrastructure Protection Plan 2013 specifically identified these innovation and research efforts as essential components of secure and resilient national infrastructure.<sup>23</sup>

The federal roles outlined in presidential guidance and interagency governance are a major first step, but most of the ICS and SCADA problem set rests in the private sector, outside of direct federal reach. The DHS, DOJ, and DOD, under the requirements of national security, lack the ability to compel action in the private sector, despite the imminent threat. Despite this, the US government does have a federal framework with which to respond to a cyber attack.

## **US Government Response Methodology**

The United States is one of only a few nations to declare possessing a formal offensive cyber capability, ostensibly to dissuade adversaries through the assurance that the United States retains freedom of action across a full-spectrum

of response options. It is important, then, to discuss the contexts within which and the processes by which the government will respond to cyberattack.

The principle that any response to cyber incidents will be the minimum sufficient force required to achieve the desired effect is central to PPD-20 and restated across all the other federal directives. This emphasis on restraint is evident by the explicit PPD-20 guidance that network defense, law enforcement options, and countermeasures all be exhausted and determined to be insufficient before consideration of cyber options.<sup>24</sup> Diplomatic activities, likely running in parallel with the other efforts, would be continually used to influence both adversarial and friendly behavior where feasible. Threat severity or timescale might preclude deliberate planning and thereby blur the lines between network defense, law enforcement, diplomacy, and other routine interagency coordination.

The classified federal cyber response construct focuses on the interagency level, but the unclassified USCYBERCOM framework incorporates similar rationale from attack characterization phase to response phase. Interagency leadership continually reevaluates each step in this process against the evolving situation, timelines, consequences, effects, and legality under domestic and international law.<sup>25</sup> The response model is designed to provide decision paths that depart the cyber realm and move into more familiar frameworks for application of traditional instruments of power. The four escalating levels of response are common to both federal and USCYBERCOM models, including inaction, denial of objectives, cost imposition, and deterrence of future attacks. Each can grow in severity, but also in required capability, risk, and burden of proof.

Conventional wisdom stresses that achieving cyber attribution is difficult to impossible. Investigations usually lead back to a compromised system, often in countries with poor diplomatic or legal connections to the United States and Internet governance bodies. Because of this it is also likely that the compromised system was chosen for targeting to impede law enforcement. “[Malicious] actors can and do operate in secrecy with substantial impunity from virtually anywhere on the planet.”<sup>26</sup> The vast majority of malicious cyber activity incidents do not receive the analytic resources needed to determine their true origins. Also, investigations conducted only within cyberspace without consideration of other domains are not likely to succeed.

Cyber attribution is rapidly improving, however. This can be seen in CrowdStrike’s Putter Panda Intelligence Report on Peoples’ Liberation Army (PLA) Unit 61486 and the DOJ’s historic indictment of PLA Unit 61398.<sup>27</sup> This new era in reporting exploits advancements in persistent analysis, reverse engineering, social media forensics, cultural and linguistics analysis, and

the expanding field of all-source analysis. Investigations of especially destructive attacks or attacks that threaten national security can extend beyond finding virtual fingerprints and doing code analysis—now incorporating digital forensics, human intelligence, physical security examinations, finance and telecommunications activity logs, and even signals intelligence. “CrowdStrike believes its report offers the final proof. ‘We’ve got the gun, the bullet and the body,’ [Adam] Meyers [CrowdStrike’s head of threat intelligence] said of evidence connecting attacks on its clients, in the space and satellite sectors, back to Unit 61486.”<sup>28</sup>

The most concerted and successful cyber attacks can exploit vulnerabilities in phases, and pursue complementary attack vectors, like spear phishing, phone calls, surveillance, and so on. Deconstruction and attribution of complex cyber attacks may require investigators to delve forensically across physical, technical, and human considerations. Multifactor, intelligence-driven approaches are essential when dealing with potential attack vectors. As demonstrated in the Aurora test, very sophisticated attacks may leave only a single IP address as a cyber fingerprint that would prove inadequate for attribution if analysis were limited to only the cyber domain.<sup>29</sup>

Real-time attribution remains the ultimate goal. However current capabilities are not up to network-speed automated responses. The technical and political challenges in actually indicting a nation-state in a case of cyber attack led to an assumption that the rapid US accusation of North Korean hackers and leadership in the 2014 Sony cyber attack would be possible only with intelligence assets in North Korea.<sup>30</sup> Nevertheless, cyber attribution methods continue to be refined. Examples of this are CrowdStrike’s litany of high-level attributions, such as the identification of the Russian “Energetic Bear” network by its resources, sophistication, and idiosyncrasies.<sup>31</sup> If defenders can couple this attribution cycle with active monitoring and future automated countermeasure capabilities, the presumption that “cyber always favors the attacker” may become challenged just as the early airpower maxim that “the bomber will always get through.”<sup>32</sup> Given the newly arrayed federal unity of effort, a discussion on the framework and likelihood of a cyber response is apt.

## **Cyber Response**

Cyber responses bearing both challenges and benefits is discussed below. Without considering the means of employment, cyber responses will aim at one or more of the following:



- observe and gain intelligence,
- deny an attack's objectives through defense and hygiene,
- neutralize the attacker and impose a proportional cost on them, or
- retaliate with a high-order response to deter future attacks.

The means of responding could include:

- hacking adversarial command-and-control infrastructure,
- interrupting network protocols,
- luring attackers into honeypot traps,
- coordinating with computer security incident response teams (CSIRT) and Internet service providers (ISP) to disrupt malicious traffic, or
- applying cyber effects to facilities or services, like ventilation or power systems, attackers rely on to execute operations.

Continuous and routine national cyber operations are hampered by the timescale challenge, access to adversary assets, crude collateral damage assessments capabilities, and an unproven history of cyber deterrence. Cyberspace is different from other domains in the sheer speed of its activities. Therefore, any related consultative process, such as an emergency national response mechanism, has to be very streamlined and adaptive to respond within an adversary's observe-orient-decide-act (OODA) loop.<sup>33</sup> Additionally, access to and exploitation of "hard" targets in advanced nation-states, might take weeks or months to accomplish. Cross-domain or covert activities might be required before being able to hold adversaries at risk. Other challenges are battle damage and collateral damage assessment for gauging precise duration and proportionality of cyber effects. Miscalculating impacts on civilians or public opinion from errant cyber-response operations could seriously damage greater strategic interests. The desired effects of cyber operations must be weighed against possible intelligence or operational gains or losses.

Existence of any real US strategic cyber deterrence is doubtful.<sup>34</sup> However attribution provided by national and private assets is accurate. Secretary of Defense Ash Carter framed the deterrence challenge, acknowledging it "requires a multi-faceted effort . . . including network defense measures, economic actions, law enforcement actions, defense posture and response capabilities, intelligence, declaratory policy and the overall resiliency of US networks and systems."<sup>35</sup> The 2014 *Blue Horizons IV* report offers that strategic cyber deterrence will ultimately not become a geopolitical reality without rapid, trusted attribution and system-of-systems scale resilience.<sup>36</sup>

However responding with and through cyberspace for effects and influencing adversarial will does provide several advantages in the adaptability of effects, the speed of action, synergistic capacity, global and immediate impact, rapid capability development, and reversible effects. Cyber operators can realize effects in the physical, virtual, cyber persona, and human dimensions, thus offering maneuver and application of force in previously unforeseen ways.<sup>37</sup> The instantaneous timescale of cyber operations becomes a vital asset on the offensive, especially when prosecuting time-sensitive targets. Ubiquitous and dual-use global cyber infrastructure also provides cover and concealment for response actions. Cyber integrates extremely well into a broader set of national tools. For example cyber strongly enhances options and capabilities when synchronized with special operations, electronic warfare, military information support operations, sanctions, or diplomatic messaging. Cyber capabilities can also be fielded rapidly with minimal acquisition cost compared to traditional weapons systems. Proponents also claim that the reversible and nonkinetic nature of cyber operations make them an extremely versatile foreign policy tools if used correctly, in an era of restraint, global news cycles, and fickle public opinion.<sup>38</sup> Ultimately cyber operations provide immediate global vigilance, reach, and power projection that are unmatched in the other domains.

The United States and its allies are consistently studying and developing new cyber capabilities, but so are their adversaries. Lawmakers are beginning to appreciate the emerging threats and are calling for unilateral action. Rep. Mike Rogers, chairman of the House Intelligence Committee, made a strong appeal for more US offensive cyber operations against malignant Russian actors.<sup>39</sup> There has been increasing emphasis in recent years upon emergency cyber exercises, which are designed to overcome the challenges and blind spots in the US government's ability to respond to malicious cyber activity. These efforts will surely one day form the basis for real-world national response capability. Cyberspace is not the only domain within or through which the United States will respond to a cyber attack on its ICS or SCADA systems, as evident in the standing ROEs referenced above. Federal planning must also integrate traditional responses with cyber responses.

### **Noncyber Response**

Federal cyber-attack response planning has wisely included the application of traditional instruments of power including kinetic and nonmilitary options depending on the situation and the nature of the attack. The noncyber methods are designed to impose costs and deter future attacks. They include,

but are not limited to escalation from official designation of wrongdoing to economic and trade sanctions, law enforcement prosecution, direct action, major combat operations, and even nuclear strike. The triggers, consequences, and risks of these noncyber paths are much more clearly and generally understood and defensible than cyber actions.

It is essential that traditional and cyber options remain linked within the national toolset. Likewise cyber must be considered as a legitimate strategic response. All of this clearly indicates that full-spectrum capabilities must be brought to bear in response to a cyber attack on our critical national infrastructure. This will be more likely to change an adversary's risk calculus. Next, the dialogue about federal roles, responsibilities, and response options must move from the realm of policy into the realms of the practical and applied for the public and private sectors.

#### Notes

1. Allen, "White House Aide Says."
2. Davis, Keynote Address.
3. Office of Public Affairs, Department of Justice, "US Charges Five Chinese."
4. PPD 21, Critical Infrastructure.
5. Williams, "Cyberspace Operations."
6. Department of Homeland Security (DHS), "National Protection and Programs Directorate."
7. PPD 21, Critical Infrastructure.
8. Davis, Keynote Address.
9. US-CERT, "National Cybersecurity and Communications Integration Center."
10. White House, "Comprehensive National Cybersecurity Initiative"; and National Cyber Security Division, DHS, and US-CERT, "Privacy Impact Assessment."
11. Industrial Control Systems Cyber Emergency Response Team Web site.
12. DHS, "Critical Infrastructure Cyber Community."
13. White and Halpert, "Executive Order."
14. National Council of Information Sharing and Analysis Centers website.
15. National Initiative for Cybersecurity Careers and Studies, "National Cybersecurity Workforce Framework."
16. White House, "Remarks as Prepared for Delivery."
17. EO 13687, Imposing Additional Sanctions.
18. PPD 21, Critical Infrastructure.
19. EO 13636, Improving Critical Infrastructure.
20. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*.
21. Parfomak, "Pipeline Cybersecurity."
22. Office of Electricity Delivery and Energy Reliability, Department of Energy, "National SCADA Test Bed."
23. DHS, "National Infrastructure Protection Plan 2013."

24. Pellerin, "DOD Readies Elements."
25. Williams, "Cyberspace Operations."
26. DOD, "United States Government Submission."
27. Alperovitch, "Changing the Asymmetry of the Fight"; and Office of Public Affairs, Department of Justice, "US Charges Five Chinese."
28. Perloth, "2nd China Army Unit Implicated."
29. Tucker, "Forget the Sony Hack."
30. Sanger and Fackler, "NSA Breached North Korean Networks."
31. Perloth, "Russian Hackers Targeting."
32. Middlemas and Barnes, *Baldwin*.
33. John Boyd, *A Discourse on Winning and Losing* (unpublished set of briefing slides), document mu43947, 1987, Document Collection, Muir S. Fairchild Research Center, Maxwell AFB, AL; and PPD 21, Critical Infrastructure.
34. Henry, et al., "Securing Cyberspace."
35. Boyd, "IT Security Shifts."
36. Geis, et al., *Blue Horizons IV*.
37. Joint Publication 3-12, *Cyberspace Operations*.
38. Morgan, discussion.
39. Tucker, "House Intel Chief Wants to Increase Cyber Attacks."

## Chapter 5

# Recommendations

*Neither government nor the private sector can defend the nation alone.*

—Pres. Barack Obama

The ability of our nation to withstand a cyber attack on its critical national infrastructure, especially under a mounting threat, depends on the development of the abilities to prevent, detect, investigate, and respond to threats. The simultaneous development of private-sector integration and international consensus is also necessary. While the government has developed clear cyber policy, it must now focus its resources on two of those primary lines of cyber-security effort for the protection of its critical national infrastructure: prevention through strong stakeholder relationships, and detection and response through public, private, and international unity of effort. It is undeniable that the United States and other advanced nations will observe an increased reliance on cyber as a foreign policy tool and that developing countries will see explosive growth in cyber capabilities.<sup>1</sup> General Hayden stated that “our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a common body of knowledge.”<sup>2</sup>

## Prevention

*Instead of just building better defenses, we must build better relationships.*

—Former FBI director, Robert S. Mueller III

The first line of effort is prevention, a preconflict phase where the government can capitalize on the momentum already under way across various sectors and institutions. Prevention also requires complementary foreign and domestic initiatives including:

- international norms of cyber behavior,
- formalized critical interdependencies,
- private-sector responsibilities in law and regulation,
- focused research into advanced cyber capabilities, and
- cyber workforce professionalization.

The United States must strive to establish an international set of norms that define both peacetime and contingency expectations for state cyber behavior, communicate clear cyber foreign policy, pursue cyber defense capacity-building measures with developing nations, and develop an international understanding of the nature of “critical infrastructure.” Building an internationally accepted framework of norms of behavior and confidence-building measures in cyberspace are foremost among these efforts. This framework will provide a new level of strategic stability in cyberspace and afford the US government freedom of action in cyberspace consistent with the nation’s principles and interests.<sup>3</sup> The interagency approved the draft cyber initiatives on peacetime norms in 2014.<sup>4</sup> The initiatives are intended for future international consideration and hold that states:

- should not perform cyber-enabled intellectual property theft for economic advantage;<sup>5</sup>
- should not attack or impair critical infrastructure;
- should not impede national computer-security-incident-response team actions; and
- should behave consistently with domestic and international laws and obligations.

These norms depend upon utilizing traditional multistakeholder Internet governance rather than state-administered models of cyberspace governance, as the key to an “open, interoperable, secure, and reliable [Internet].”<sup>6</sup> While such structure implies US unilateral influence may become more diffuse, it reinforces the spirit and character of the Internet.

While the UN and NATO have outlined the initial response frameworks for major cyber attacks, the United States must continue developing and framing adequate prevention measures for the continuous below-response-threshold malicious cyber activity that occurs all over the Internet. If network defense and law enforcement mechanisms are not sufficient to mitigate and respond to threats, then the US government will examine cyber, economic, and kinetic options. While establishing international norms provides a starting point, manifesting critical interdependencies among nations and organizations reinforces the open and borderless landscape that is cyberspace.

The DOS will also continue to work toward an international consensus that defines the nature of *critical national infrastructure*. This consensus would be an important pretext to further dialogue on international norms of cyber behavior. An important corollary to this discussion of critical infrastructure is that domestic US sectors must work to understand the international depen-

dencies they rely on for operations and link to the interagency community for situational awareness and further systems-of-systems analyses.

To capture some of these critical dependencies, the DOS will continue to support multilateral cybersecurity capability building and an innovative and cooperative cyberspace environment through venues like the UN, NATO, European Union, African Union, and Organization for Security and Cooperation in Europe. Shared threat warnings, continual international engagement, confidence-building measures, and bilateral or multilateral training all can provide ways to strengthen the interoperability and trust among nations including developing countries.<sup>7</sup> These relationships are essential for detecting cybercrime, cyberespionage, and cyberwarfare; sharing law enforcement evidence; identifying cross-border dependencies; and developing new ways to attribute elusive actors.

Prevention does not rely solely on the international and domestic governance but also on the relationship between public and private cyber agencies. There have been great improvements in coordination, but continued emphasis through revised legislation, formalization of public-private relationships, and regulatory adherence to standards is required. The US government recognizes that the “key to success lies in the public-private partnership.”<sup>8</sup> However it can no longer afford to leave this to ad hoc arrangements or free market forces that have failed to induce secure and resilient strategies into the C-suite.

The first step begins with Congress passing the White House’s January 2015 cybersecurity legislation. The proposal has evolved with industry inputs since 2009 and attempts to formalize and improve the critical public-private relationship at the heart of our infrastructure.<sup>9</sup> Unlike the draft cybersecurity legislation of 2012, the more recent administration efforts recognize the need for sector-specific regulation rather than a single umbrella agency responsible across all of the cyberspace.<sup>10</sup> The recent cybersecurity bill also addresses many of the missing elements of a more robust information sharing between the public and private sectors including liability and proprietary information protection from disclosure.<sup>11</sup> This cybersecurity proposal falls during a historic confluence between a publicly acknowledged threat and unprecedented political will to create a whole-of-nation response.

The next step involves legislating new mandatory technological, administrative, and personnel standards, as identified in EO 13636, for organizations responsible for critical infrastructure. These entities should:

- formally recognize the NIST Cybersecurity Framework as the defining set of best practices in securing CI/KR;
- participate in the C3VP and ICSJWG;

- undertake DHS-led cybersecurity certification and routine assessment;<sup>12</sup> and
- provide controlled disclosure to DHS of cyber incident forensics.<sup>13</sup>

Interactive participation, assessment mechanisms, and robust two-way information sharing would serve to augment the NIST Framework, and may help companies avert an overreliance on checklists. Sincere private participation across public and private sectors is fundamental in order to assist the government in determining whether the NIST Cybersecurity Framework and broader efforts are indeed operationally effective and to ensure that these tools are living documents adapting with industry and technology.<sup>14</sup>

Each private critical sector must ultimately have mandatory regulation for mitigating risk being transferred to the national infrastructure. This regulation should be prioritized because cross-domain cyber and physical security is the essence of corporate due diligence. Existing sector efforts are useful but need improvement; the levels of effectiveness vary widely across sectors. Companies often still need modernized management practices, greater enterprise awareness, dynamic risk assessment frameworks,<sup>15</sup> intrusion protection and data loss prevention systems, identity management schemes, supply-chain monitoring, security-oriented acquisition, red-team capabilities, and other support measures for maximum cybersecurity program effectiveness. Many sectors could look to the financial sector, which has developed a behavioral profile and big data analytics to counter insider threats that could be paradigmatic for other sectors. There should also be questioning of how much control systems interface with business and other IT networks, because they are often the easiest to compromise by exploiting poor cyber hygiene or user behavior.

There are also several possibilities for due diligence and information sharing to increase cybersecurity by using corporate incentives and transferred legal constructs. Demonstrating successful adherence to the NIST Cybersecurity Framework could result in corporate tax or insurance rate subsidies to defray business costs. Failure to do so could result in fines. The needs for disclosure of cybersecurity incident data and protection of corporate interests might be reconciled by a process akin to the workings of the US Foreign Intelligence Surveillance Court. In this way a legally defensible and secure disclosure system might be built.

Changes like these would be highly contentious due to increased regulation, but they might achieve sufficient levels of cybersecurity across *all* the critical sectors before existential threats arise. The challenge of securing critical infrastructure spans virtual and physical domains. Private-sector needs of



convenience, uptime, and profits compete with national needs for security, testing, and resilience.

The firing of Target's chief executive officer due to the major 2014 compromise represents an inflection point where the private sector began to link pay and employment in the C-suite to cybersecurity performance.<sup>16</sup> Threats and technology are moving light years faster than cybersecurity and fail to induce corporate behavior change. This is especially true outside of the relatively self-motivated financial and energy sectors. Retired general Hayden warned that "cyber defense is not a subtraction from the bottom line. Rather it is an integral and essential element in creating the top line."<sup>17</sup>

The federal government should continue to find new and innovative ways to increase sharing of real-time information with critical infrastructure owners while ensuring information classification restrictions do not inhibit the intelligence sharing essential to the cyber safety and resilience. President Obama provided direction for these efforts in the February 2015 Cybersecurity Summit, the subsequent Executive Order 13691 on Information Sharing, and the creation of voluntary information sharing and analysis organizations (ISAO). The president also expanded on the current sector-delimited ISAC model and encouraged consensus building and shared cybersecurity awareness across subsector to cross-sector and public- to private-sector lines.<sup>18</sup> The interaction between DHS and the ISAOs will be based on voluntary standards for automated information sharing with the government providing qualified ISAOs with federal liability protection from cyber incident disclosure.

DHS should examine what and with whom it shares critical cyber intelligence. Threat data must include not only indicators but also the maximum intelligence possible—assuring that it is secure and actionable. Critical infrastructure operators should also have cleared liaison personnel within the NCCIC as provided for under section 4(c) of the EO 13691.<sup>19</sup> That could help eliminate traditional barriers to communication, advocate for rapid declassification of threat intelligence, and ensure that automated information sharing channels like STIX™/TAXII™ are as developed or refined as possible.

DHS should continue developing capabilities to fuse physical and cyber infrastructure situational awareness for a holistic understanding of their interdependencies and potential cascading effects between systems and sectors, for the government and for corporations.<sup>20</sup> DHS should continue to seek and champion ICS and SCADA systems cybersecurity best practices—such as those developed by ICS-CERT—to provide automatic vulnerability and mitigation recommendations.<sup>21</sup> DHS must also ensure the NIST Cybersecurity Framework remains as adaptable and dynamic as are the threats to our critical infrastructure. Finally, in the long-term, DHS may consider transitioning

the Cybersecurity Framework to a nongovernmental entity in the spirit of open and inclusive participation. This might be similar to the gradual shift in Internet governance and oversight from the Department of Commerce to the Internet Corporation for Assigned Names and Numbers (ICANN).<sup>22</sup>

A highly trained and professionalized cybersecurity corps is the heart of effective cybersecurity. The DHS should continue to lead and expand cybersecurity workforce professionalization efforts like NICE. In the same vein, the government should pursue and invest in cyber ranges and simulation exercises. These facilities could promote the integration of DHS, FBI, and DOD experts with ICS and SCADA cybersecurity staffs to train and exercise skills in a permissive environment with realistic feedback. As General Davis remarked, “[Long-term] institutional capability in cyberspace is about building the right kind of people, including leaders, who truly understand what [cyber] is about, and who can apply the intellectual staying power to secure an advantage for the future.”<sup>23</sup>

The federal government must continue to fund and expand the work of the DOE at the National SCADA Test Bed, the leading effort to bring innovation, cybersecurity, and standards to our critical sectors, which can then be disseminated to private industries. The work conducted within the national labs is the seed corn that will bear true fruit in years to come. From that seed will come key advances in integrated physical and cyber sensor technologies, big data and predictive analytics, trusted supply-chain initiatives, anomalous behavior detection (including power profiling), and secure life-cycle system acquisition and design. However, despite the best layered-security integrating technology with a well-educated workforce, a determined adversary will eventually find an exploitable attack surface and activities must shift from prevention to mitigation.

## **Detection and Response**

*Cyber is chess, not solitaire, as the adversary always has a move.*

—Dmitri Alperovitch  
co-founder and chief  
technology officer, CrowdStrike

The reality is that static defense concedes the element of surprise to adversaries. Nevertheless the government can improve detection and response capabilities in vulnerable sectors with advanced automated tools and sensors, an emphasis on private-sector incident responses, private-sector intelligence

sharing, and realistic national cyber-response training and exercises. The current challenge in cybersecurity is in decreasing the time between compromise and detection—from years to fractions of seconds.<sup>24</sup> Diminishing the interval between identifying, assessing, and then mitigating the malicious activity that will inevitably get through and internal compartmentalization of the more critical mission areas for mission assurance are the necessary elements of cyber resilience.

Automated tools, operating at network speeds across machine-to-machine interfaces are vital for defenders to detect and describe malicious activity, deduce adversaries' objectives, and provide authorities with response options amid the pervasive fog of war. The DHS, acting with new legal and regulatory authorities, in concert with sector-specific agencies, should deploy a sensor system analogous to the Einstein 2/3A program across CI/KR enterprises to provide automated detection capability, intrusion protection, and decision-quality intelligence, underpinned by analysts well trained in ICS and SCADA cybersecurity. Beyond technology, the DHS and its ICS-CERT arm should ensure strong linkage with private sector SOCs, with their continuous monitoring and organic incident response mechanisms, while providing aid to organizations in the formal development of cyber continuity of operations planning (COOP).

Linking federal cyber, intelligence, and law enforcement capabilities with the critical infrastructure sectors in an effective manner, as outlined in PPD-21, also represents one of the few feasible strategies to countering our adversaries' asymmetric offensive cyber advantage. Cross-organizational threat information sharing, proactive assessments, next-generation endpoint detection and prevention technologies, strengthened internal security controls,<sup>25</sup> increased priority for corporate security clearances, and greater cross-flow of industry experts through government positions are necessary for improving our abilities to identify anomalous behavior and detect broader threat streams. Organizations that experience cyber attacks must report them to the DHS Protected Critical Infrastructure Information Program.<sup>26</sup> Cyber-attack data is critical to infrastructure cyberhealth awareness. The DHS must protect this extraordinarily proprietary information from accidental release or legal discovery. However, the financial sector has experienced that there is no competitive advantage in hoarding sector cybersecurity information because competitors are certain to be victims of the same or similar attacks, and therefore, cybersecurity transparency is actually an existential requirement.

There are also established international information sharing channels that support domestic and international cybersecurity. These channels must remain prioritized, coordinated where needed, and frequently exer-

cised, and include diplomatic (DOS-to-ministries of foreign affairs), law enforcement (legal attachés-to-ministries of justice and interior), technical (CERT-to-CERT), and the liaisons between the various national intelligence services. These relationships represent myriad potential opportunities for engagement with international partners and with adversaries as well. These relationships can reinforce cyber due diligence across the international community, help address the challenges of threats coming from extraterritorial malicious actors, and provide greater resources for the protection of the average Netizen. Critical US infrastructure also exists outside of the territory of the United States—DOD-operated facilities in allied countries or simply foreign infrastructure supporting US activities. Relationships with foreign host governments, their CERTs, and IT companies are invaluable as adversaries seek softer targets that underpin the ability to project US interests abroad.

Finally, the White House and interagency community must continue to exercise routine national cyber emergency scenarios to refine the speed of response, ensure realistic scenarios extend beyond the cyber realm, and draw upon expertise in the industrial, emergency management, and other effected sectors. Major federal response resembles an “emergency conferencing procedure that links key organizations and leaders from across the DOD and the government, to quickly assess major cyber threats and make decisions, much like we do for any major physical threat to the nation.”<sup>27</sup> Basically, the US government must ensure response activities remain top priorities through turbulent funding cycles and ensure collaboration never succumbs to bureaucratic inertia.

#### Notes

1. Daniel, Holleyman, and Niejelow. “China’s Undermining an Open Internet.”
2. Hayden, “Future of Things ‘Cyber.’”
3. Morgan, discussion.
4. Tom Dukes, deputy coordinator for cyber issues, Office of the Secretary, Department of State, to the author, e-mail, 8 August 2016.
5. Daniel, Holleyman, and Niejelow, “China’s Undermining an Open Internet.”
6. Davis, Keynote Address.
7. Morgan, discussion.
8. Ibid.
9. White House, “Remarks by the President.”
10. Lewis, Center for Strategic and International Studies (CSIS), Testimony.
11. Swisher, “Kara Swisher Interviews President.”
12. EO 13636, Improving Critical Infrastructure.
13. Dilanian, “NSA Director.”
14. Lewis, CSIS Testimony.

15. Parfomak, "Pipeline Cybersecurity: Federal Policy."
16. Riley, et al., "Missed Alarms."
17. Bhimani, "Cyber-Security."
18. EO 13691, Promoting Private Sector Cybersecurity.
19. Ibid.
20. PPD 21: Critical Infrastructure.
21. ICS-CERT website.
22. Hyman, "US to Scale Back Its Role."
23. Davis, Keynote Address.
24. Ibid.
25. Alperovitch, "New Era of Cyber Attacks."
26. CS-CERT website.
27. Davis, Keynote Address.



## Chapter 6

# Conclusion

*Protecting our digital infrastructure is a national security priority.*

—Pres. Barack Obama

Realizing modern cybersecurity across US critical national infrastructure is a shared responsibility between public and private sectors. Much of the remaining work is in shaping international consensus on norms of state cyber behavior, enforcing private-sector responsibilities that affect US national interests, and continual investment and effort in refining the interagency leadership in this rapidly changing space. The rise in sophistication and frequency of cyber attacks, especially against critical sectors, coupled with antiquated and inadequate security practices and the risks from increasing global interconnectivity all demand national unity of effort and international cooperation and consensus to overcome. Government and corporate leaderships must greatly improve their willingness to receive, process, and decisively act on bad news. Unlike the exploitation of retailers for credit card information or hacktivist defacement of websites, the physical and virtual effects experienced from cyber attacks on the ICS or SCADA systems operating our core industries represent a great danger demanding nonpartisan, whole-of-government effort to preserve the American way of life. This issue is of a magnitude that it should no longer be vulnerable to the corporate lobbies, congressional agendas, or bureaucratic inertia. The fate of our nation depends on our ability to work together for the protection of these systems and the national greater good.





## Abbreviations

C3VP	Critical Infrastructure Cyber Community Voluntary Program
CI/KR	critical infrastructure and key resources
CISCP	Cyber Information Sharing and Collaboration Program
COOP	continuity of operations planning
CRG	Cyber Response Group
CSIRT	computer security incident response team
C-suite	senior management
CTIIC	Cyber Threat Intelligence Integration Center
DDOS	distributed denial-of-service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
ECS	Enhanced Cybersecurity Services
EO	Executive Order
FBI	Federal Bureau of Investigation
FLASH	FBI Liaison Alert System
HVAC	heating-ventilation-air-conditioning
IC	intelligence community
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
ISAC	information sharing and analysis center
ISAO	information sharing and analysis organizations
ISP	Internet service provider

IT	information technology
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
NERC	North American Electric Reliability Corporation
NICE	National Institute for Cybersecurity Education
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate of the DHS
NSA	National Security Agency
OODA Loop	observe-orient-decide-act loop
PLA	Peoples' Liberation Army (China)
PPD-21	Presidential Policy Directive 21, Critical Infrastructure Security and Resilience.
Project SHINE	SHodan INtelligence Extraction
ROE	rules of engagement
S/CCI	coordinator for cyber issues at the Department of State
SCADA	supervisory control and data acquisition
SLTT	state, local, tribal, and territorial
SOC	security operations center
STIX™	Structured Threat Information eXpression
TAXII™	Trusted Automated eXchange of Indicator Information
UN	United Nations
UNGGE	UN Group of Governmental Experts
US-CERT	US Cyber Emergency Response Team
USCYBERCOM	US Cyber Command

## Bibliography

- Allen, Jonathan. "White House Aide Says Cyber Response Group Protects Business." *The Washington Post–Bloomberg*, 10 December 2014. Accessed 24 March 2015. <http://washpost.bloomberg.com/Story?docId=1376-NG-DMWG6JTSE901-0N6IUQP1J26MONTLFG9FF69I7O>.
- Alperovitch, Dmitri, co-founder and the chief technology officer of CrowdStrike. "Changing the Asymmetry of the Fight in Cyberspace." Address. *United States Army Cyber Talks: Critical Issues in Cyber Operations*. The Army Cyber Institute at West Point and the US Army Cyber Command. Lincoln Hall Auditorium, National Defense University, Ft. Lesley J. McNair, Washington, DC, 30 September 2014. <https://www.youtube.com/watch?v=rZ1vPXK2bTA&list=PLtUuPz3a0Gz-0OST5wgMIMryzP1AOZQBH&index=2>.
- . "New Era of Cyber Attacks—Know Thy Adversary." *CrowdStrike* (blog), 23 December 2014. Accessed 7 January 2015. <http://blog.crowdstrike.com/new-ea-cyber-attacks-know-thy-adversary>.
- Assante, Michael, director of SANS ICS. "ICS/SCADA Security Challenges and Developments." Address. *United States Army Cyber Talks: Critical Issues in Cyber Operations*. The Army Cyber Institute at West Point and the US Army Cyber Command. Lincoln Hall Auditorium, National Defense University, Ft. Lesley J. McNair, Washington, DC, 30 September 2014. <https://www.youtube.com/watch?v=5ZtthSuwvV0&list=PLtUuPz3a0Gz-0OST5wgMIMryzP1AOZQBH&index=9>.
- Bhimani, Anish. "Cyber-Security: Fear This, Not That." *Thought*, Spring 2014, 2–4. Accessed 4 February 2015. [https://www.jpmorgan.com/directdoc/is\\_thought\\_1q2014.pdf](https://www.jpmorgan.com/directdoc/is_thought_1q2014.pdf).
- Boyd, Aaron. "IT Security Shifts from Prevent to Resiliency." *Federal Times*, 22 September 2014. Accessed 22 October 2014. <http://www.federaltimes.com/apps/pbcs.dll/article?AID=2014309220008>.
- . "SecDef "Nominee: Cyber Threats Require Holistic Defense Strategy." *Federal Times*, 4 February 2015. Accessed 6 February 2015. <http://www.federaltimes.com/story/government/cybersecurity/2015/02/04/cyber-part-broad-defense-strategy/22869325/>.
- Document Collection. Muir S. Fairchild Research Center, Maxwell AFB, AL. Clausewitz, Gen Carl von. *On War*. Translated by Col J. J. Graham. Dorset, UK: Dorset Press, 25 February 2006.
- Cloherly, Jack. "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad.'" *ABC News*, 22 May 2012. Accessed 18 September 2014. <http://abc>

[news.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875](http://news.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875).

- Daniel, J. Michael, Robert Holleyman, and Alex Niejelow. "China's Undermining an Open Internet: We Must Work Together on Reliable Cybersecurity." *Politico*, 4 February 2015. Accessed 6 February 2015. <http://www.politico.com/magazine/story/2015/02/china-cybersecurity-14875.html#.VNYJOJ2opcY>.
- Davis, Maj Gen John A., USA. Keynote Address. Armed Forces Communications and Electronics Association International Cyber Symposium. Baltimore, MD: Defense Video and Imagery Distribution System, 2013. [http://www.dvidshub.net/video/294716/mg-davis-afcea#.VD\\_u0vIbV8E](http://www.dvidshub.net/video/294716/mg-davis-afcea#.VD_u0vIbV8E).
- Department of Defense. "United States Government Submission to the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012–2013," 2012. <http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Seminar%20on%20CBMs%20in%20Cyberspace,%20Seoul,%202011-12September2012/Annex%20J%20-%20United%20States%20Submission%20to%20the%20UNGGE%20on%20ICT%20Security%202012.pdf>.
- Department of Homeland Security (DHS). "Critical Infrastructure Cyber Community C3 Voluntary Program." DHS. Accessed 19 October 2014. <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program>.
- . "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience." DHS.gov, 2013. Accessed 23 January 2015. [http://www.dhs.gov/sites/default/files/publications/NIPP%202013\\_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience\\_508\\_0.pdf](http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf).
- . "National Protection and Programs Directorate at a Glance." DHS.gov, June 2014. Accessed 26 March 2015. <http://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf>.
- Dilanian, Ken. "NSA Director: Yes, China Can Shut Down Our Power Grids." *Business Insider*, 20 November 2014. Accessed 21 November 2014. [http://www.businessinsider.com/nsa-director-yes-china-can-shut-down-our-power-grids-2014-11?utm\\_content=bufferbafcd&utm\\_medium=social&utm\\_source=facebook.com&utm\\_campaign=buffer](http://www.businessinsider.com/nsa-director-yes-china-can-shut-down-our-power-grids-2014-11?utm_content=bufferbafcd&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer).
- Executive Order 13636. Improving Critical Infrastructure Cybersecurity, 12 February 2013. Accessed 22 October 2014. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- 13687. Imposing Additional Sanctions with Respect to North Korea, 2 January 2015. Accessed 22 January 2015. <http://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea>.
- 13691. Promoting Private Sector Cybersecurity Information Sharing, 13 February 2015. Accessed 26 February 2015. <http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- Flynn, Sheila, Department of State Office of the Coordinator for Cyber Issues. Presentation. "International Cyberspace Security and Strategy." Department of State Tour for Air Force Fellows, Washington, DC, 2014.
- Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare." NATO Cooperative Cyber Defence Centre of Excellence BlackHat Japan 2008 Symposium. Tokyo, 2008. <http://blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf>.
- Geis, Col John P., USAF, retired, PhD, Grant T. Hammond, PhD, and Harry A. Foster. "Blue Horizons IV: Deterrence in the Age of Surprise." CSAT Occasional Paper 70. Maxwell AFB, AL: Air University Press, 2014.
- Glazer, Emily. "J. P. Morgan CEO: Cybersecurity Spending to Double." *The Wall Street Journal*, 10 October 2014. Accessed 4 February 2015. <http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976>.
- Gorman, Siobhan. "Electricity Grid in US Penetrated by Spies." *The Wall Street Journal*, 8 April 2009. Accessed 24 September 2014. <http://online.wsj.com/article/SB123914805204099085.html>.
- Hagel, Chuck, secretary of defense. "Defense Innovation Days." Keynote address. Southeastern New England Defense Industry Alliance, Middletown, RI, 3 September 2014. Accessed 17 September 2014. <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1877>.
- Hayden, Gen Michael V., USAF, retired. "The Future of Things 'Cyber'." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3–7.
- Henry, Shawn, David Sanger, and James Andrew Lewis with Bob Schieffer. "Securing Cyberspace: A Discussion on the Sony Hack Plus the Latest Threats." Schieffer Series Dialogues. Center for Strategic and International Studies, Washington, DC, 21 January 2015. <http://www.youtube.com/watch?v=eaKvMk4ujEM> and [https://csis-prod.s3.amazonaws.com/s3fs-public/event/150121\\_Schieffer\\_Securing\\_Cyberspace.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/event/150121_Schieffer_Securing_Cyberspace.pdf).

- Hyman, Leonard. "US to Scale Back Its Role in Internet Governance." *Tech Crunch*, 19 February 2015. Accessed 24 March 2015. <http://techcrunch.com/2015/02/19/1120736/>.
- Industrial Control Systems Cyber Emergency Response Team website. Accessed 19 October 2014. <https://ics-cert.us-cert.gov>.
- . ICS-CERT Advisory (ICSA-11-084-01). "Solar Magnetic Storm Impact on Control Systems," 26 March 2011. Accessed 20 April 2015. <https://ics-cert.us-cert.gov/advisories/ICSA-11-084-01>.
- InfraGard website. Accessed 23 October 2014. <https://www.infragard.org>.
- Inglis, John C., deputy director, National Security Agency. "National Security Agency/Central Security Service Core Values: Q&A with NSA's Deputy Director." *Intelligence Community on the Record*, 15 January 2009. Accessed 16 October 2014. <http://icontherecord.tumblr.com/post/58823372345/national-security-agency-central-security>.
- Joint Publication 3-12, *Cyberspace Operations*, 5 February 2013.
- Kaspersky Lab. "The Regin Platform: Nation-State Ownage of GSM Networks." *Kaspersky Lab Reports*, 24 November 2014. Accessed 8 January 2015. [http://securelist.com/files/2014/11/Kaspersky\\_Lab\\_whitepaper\\_Regin\\_platform\\_eng.pdf](http://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf).
- Kovacs, Eduard. "Cyberattack on German Steel Plant Caused Significant Damage: Report." *Security Week*, 18 December 2014. Accessed 15 January 2015. <http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report>.
- Lewis, James A., Center for Strategic and International Studies. Testimony before the Senate Committee on Commerce, Science and Transportation. *Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework*. 114th Congress, 1st sess., 4 February 2015. [http://www.commerce.senate.gov/public/index.cfm/hearings?Id=eb8d0d69-bf71-4052-9675-ad6d4c507782&Statement\\_id=BA87C0A0-050E-4A5C-8E94-72700092FCC3](http://www.commerce.senate.gov/public/index.cfm/hearings?Id=eb8d0d69-bf71-4052-9675-ad6d4c507782&Statement_id=BA87C0A0-050E-4A5C-8E94-72700092FCC3).
- Libicki, Martin C. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly* 5, no 1 (Spring 2011): 132–46.
- Martin, Michelle, and Erik Kirschbaum. "Pro-Russian Group Claims Cyber Attack on German Government Websites." *Reuters*, 7 January 2015. Accessed 8 January 2015. <http://www.reuters.com/article/2015/01/07/us-germany-cyberattack-idUSKBN0KG15320150107>.
- Middlemas, Keith, and John Barnes. *Baldwin: A Biography*. London: Macmillan, 1970.

- Minkel, J. R. "The 2003 Northeast Blackout—Five Years Later." *Scientific American*, 13 August 2008. Accessed 11 November 2014. <http://www.scientificamerican.com/article/2003-blackout-five-years-later>.
- Mueller, Robert S, III. "Remarks: The Cyber Threat—Planning for the Way Ahead." *FBI.gov*, 28 February 2013. Accessed 11 October 2014. <http://www.fbi.gov/news/stories/2013/february/the-cyber-threat-planning-for-the-way-ahead>.
- Nakashima, Ellen. "Iran Blamed for Cyberattacks on US Banks and Companies." *The Washington Post*, 21 September 2012. Accessed 4 February 2015. [http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312\\_story.html](http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html).
- National Council of Information Sharing and Analysis Centers website. Accessed 26 March 2015. <http://www.isaccouncil.org/aboutus.html>.
- National Cyber Security Division (NCSD), Department of Homeland Security, and United States Computer Emergency Readiness Team. "Privacy Impact Assessment, EINSTEIN Program: Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government." Includes 2016 Privacy Impact Assessment Three-Year Review. *DHS.gov*, September 2004. Accessed 15 October 2014. [https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein-june2013-3-year-review\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein-june2013-3-year-review_0.pdf).
- National Initiative for Cybersecurity Careers and Studies (NICCS). "National Cybersecurity Workforce Framework." NICCS. Accessed 15 January 2015. <http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework>.
- North American Electric Reliability Corporation. *Critical Infrastructure Protection Standards*. *NERC.com*. Accessed 8 January 2015. <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>.
- North Atlantic Treaty Organization (NATO). "Wales Summit Declaration." Press release, 5 September 2014. [http://www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](http://www.nato.int/cps/en/natohq/official_texts_112964.htm).
- Office of Electricity Delivery and Energy Reliability, Department of Energy. "National SCADA Test Bed." *Energy.gov*. Accessed 19 October 2014. <http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed>.
- Office of Public Affairs, Department of Justice. "US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage." *Justice.gov*, 19 May 2014. Accessed 15 October 2014. <http://www.justice.gov/opa/pr/us-charges>

five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

- Parfomak, Paul. *Pipeline Cybersecurity: Federal Policy*. Congressional Research Service (CRS) R42660. Washington, DC: CRS, 16 August 2012.
- Pellerin, Cheryl. "DOD Readies Elements Crucial to Cyber Operations." *American Forces Press Service*, 27 June 2013. <http://archive.defense.gov/news/newsarticle.aspx?id=120381>.
- Perlroth, Nicole. "2nd China Army Unit Implicated in Online Spying." *The New York Times*, 9 June 2014. Accessed 30 September 2014. <http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?ref=technology&r=0>.
- . "New Security Report Confirms Everyone is Spying on Everyone." *The New York Times*, 22 January 2014. Accessed 14 October 2014. [http://bits.blogs.nytimes.com/2014/01/22/new-security-report-confirms-everyone-is-spying-on-everyone/?\\_php=true&\\_type=blogs&r=2](http://bits.blogs.nytimes.com/2014/01/22/new-security-report-confirms-everyone-is-spying-on-everyone/?_php=true&_type=blogs&r=2).
- . "Russian Hackers Targeting Oil and Gas Companies." *The New York Times*, 30 June 2014. Accessed 25 September 2014. <http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html>.
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, 12 February 2013. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- Rashid, Fahmida Y. "Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems." *Security Week*, 6 October 2014. Accessed 19 October 2014. <http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems>.
- Reilly, Steve. "Bracing for a Big Power Grid Attack: 'One Is Too Many'" *USA Today*, 24 March 2015. Accessed 24 March 2015. <http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/>.
- Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg Business*, 13 March 2014. Accessed 17 February 2015. <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>.
- Sanger, David, and Martin Fackler. "NSA Breached North Korean Networks Before Sony Attack, Officials Say." *The New York Times*, 18 January 2015. Accessed 18 January 2015. <http://www.nytimes.com/2015/01/19/world/>



asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?\_r=1.

- Swearingen, Michael, Steven Brunasso, Joe Weiss, and Dennis Huber. "What You Need to Know (And Don't) About the AURORA Vulnerability." *Power Magazine*, 1 September 2013. Accessed 15 January 2015. <http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?pagenum=1>.
- Swisher, Kara. "Kara Swisher Interviews President Barack Obama on Cyber Security, Privacy and His Relationship with Silicon Valley" *Recode.net*, 13 February 2015. <http://recode.net/2015/02/13/barack-obama-recode-kara-swisher-video>.
- Taylor, Guy. "James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to US." *The Washington Times*, 26 February 2015. Accessed 5 April 2015. <http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all>.
- Tucker, Patrick. "Forget the Sony Hack, this Could Be the Biggest Cyber Attack of 2015." *Defense One*, 19 December 2014. Accessed 8 January 2015. <http://www.defenseone.com/technology/2014/12/forget-sony-hack-could-be-he-biggest-cyber-attack-2015/101727/?oref=d-dontmiss>.
- . "House Intel Chief Wants to Increase Cyber Attacks Against Russia." *Defense One*, 2 October 2014. Accessed 8 October 2014. <http://www.defenseone.com/politics/2014/10/house-intel-chief-wants-increase-cyber-attacks-against-russia/95675/>.
- United Nations (UN) Group of Governmental Experts. "Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)." UN General Assembly, 68th Session, 2013. [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/98](http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98).
- United States Computer Emergency Response Team (US-CERT). "National Cybersecurity and Communications Integration Center." US-CERT. Accessed 26 February 2015. <https://www.us-cert.gov/nccic>.
- Vego, Milan. *Joint Operational Warfare: Theory and Practice*. Newport, RI: US Naval War College, 2009.
- Wagstaff, Jeremy. "All at Sea: Global Shipping Fleet Exposed to Hacking Threat." *Reuters*, 23 April 2014. Accessed 11 November 2014. <http://www.reuters.com/article/2014/04/23/us-cybersecurity-shipping-idUSBREA3M20820140423>.
- Warden, Col John A, III. "Employing Air Power in the Twenty-First Century." In *The Future of Air Power in the Aftermath of the Gulf War*, edited by Richard H. Shultz Jr. and Robert L. Pfaltzgraff Jr., 57–82. Maxwell AFB, AL: Air University Press, 1992.

- White, Sydney, and Jim Halpert. "Executive Order 'Promoting Private Sector Cybersecurity Information Sharing': Top Points." DLA Piper, 26 February 2015. Accessed 26 March 2015. <https://www.dlapiper.com/en/us/insights/publications/2015/02/executive-order-private-sector-cybersecurity-info/>.
- The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011. Accessed 18 December 2014. [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).
- . "Remarks as Prepared for Delivery by Assistant to the President for Homeland Security and Counterterrorism Lisa O. Monaco—Strengthening our Nation's Cyber Defenses." The White House website, 11 February 2015. Accessed 19 February 2015. <http://www.whitehouse.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun>.
- . "Remarks by the President at the National Cybersecurity Communications Integration Center." The White House website, 13 January 2015. Accessed 15 January 2015. <http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent>.
- . "The Comprehensive National Cybersecurity Initiative." WhiteHouse.gov. <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.
- Williams, Maj Gen Brett T., USAF. "Cyberspace Operations." Address. 18th International Command and Control Research and Technology Symposium. Washington, DC, 2013.
- World Nuclear Association (WNA). "Fukushima Accident." WNA, February 2015. Accessed 20 April 2015. <http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/fukushima-accident/>.
- Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, 3 November 2014. Accessed 11 November 2014. <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet>.



AIR UNIVERSITY PRESS

<http://www.au.af.mil/au/aupress/>



ISBN 978-1-58566-276-0  
ISSN 2329-5821