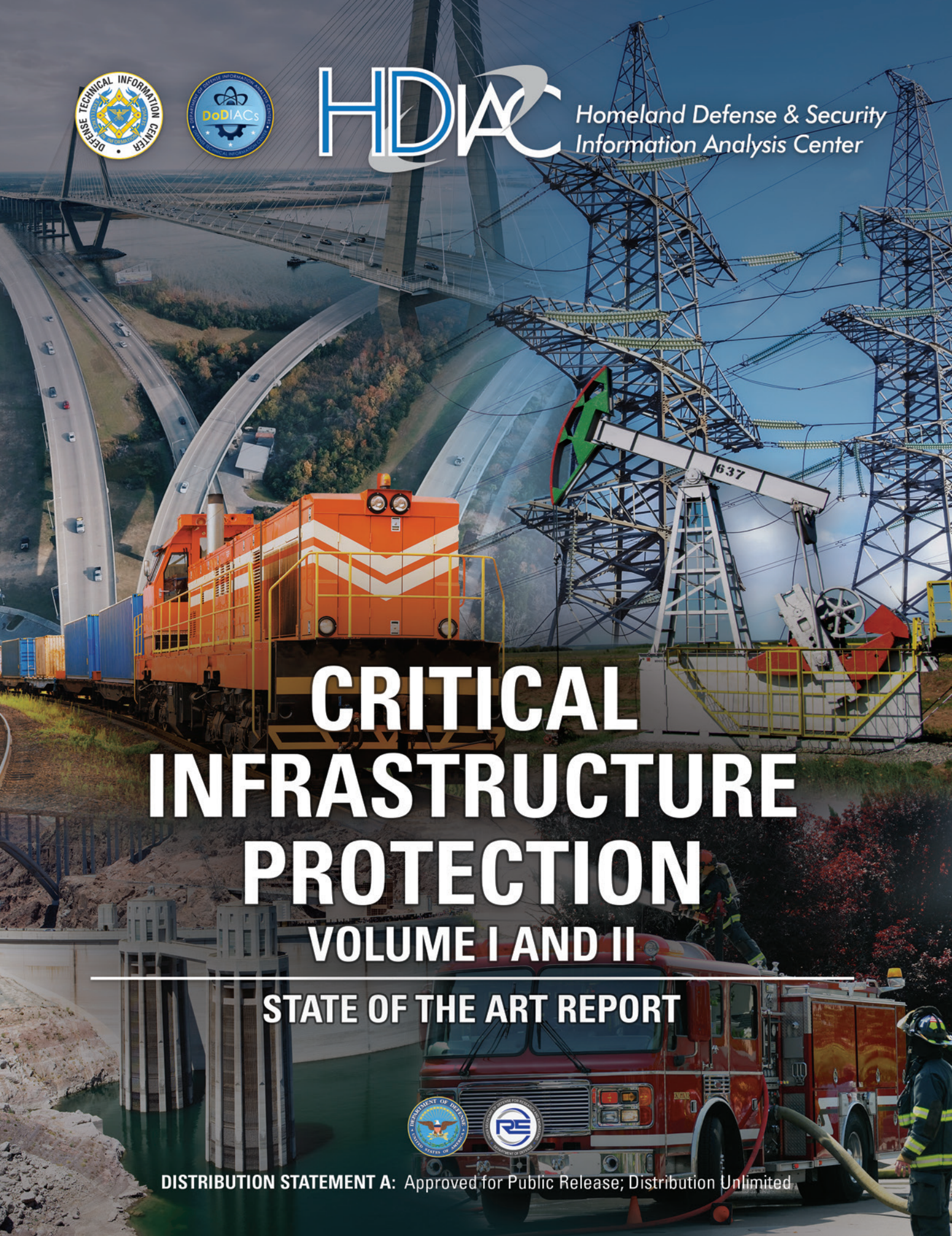

CRITICAL INFRASTRUCTURE PROTECTION

VOLUME I AND II

STATE OF THE ART REPORT

DISTRIBUTION STATEMENT A: Approved for Public Release; Distribution Unlimited

STATE OF THE ART REPORT:

Critical Infrastructure Protection

Patrick Baxter, George Mason University
Nathanael Bocker, LateralUs, LLC
Jeth Fogg, Ph.D., North American Aerospace Defense Command / U.S. Northern Command
Tyler Goodwin, George Mason University
Anura P. Jayasumana, Ph.D., Colorado State University
Tonya E. Thornton, Ph.D., George Mason University
Dirk Plante, Homeland Defense & Security Information Analysis Center
Steve Redifer, Homeland Defense & Security Information Analysis Center
Aleksandra Scalco, Naval Information Warfare Center – Atlantic
Steve Simske, Ph.D., Colorado State University
David Weissman, Colorado State University

March 05, 2021

Contract Number: FA8075-19-DA001

SPONSORSHIP STATEMENT:

The Homeland Defense & Security Information Analysis Center (HDIAC) is a Department of Defense (DOD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY. Reference herein to any specific commercial products, process, or service by tradename, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the HDIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the HDIAC, and shall not be used for advertising or product endorsement purposes.

ABOUT THIS PUBLICATION:

This State of the Art Report (SOAR) is published by Quanterion Solutions Incorporated under HDIAC contract FA8075-19-DA001. The government has unlimited free use of and access to this publication and its contents both print and electronic versions. Information presented in this SOAR may be reproduced as long as the following message is noted: "This article was originally published in the HDIAC SOAR: Critical Infrastructure Protection, 2021." This publication is also available online at https://www.hdiac.org

ABOUT THE COVER:

Cover Graphic Composite: Shelley Stottlar, Quanterion Solutions, Inc., featuring Deposit Photos from ekina1, sframe, dotsent, dedivan1923, digital94086; Unsplash Photos from davidmartinjr.

Distribution Statement A: Approved for Public Release; Distribution Unlimited

Table of Contents

List of Figures

List of Tables

About the Authors

Patrick Baxter

George Mason University

Patrick Baxter is a Public Policy Ph.D. student (Econometric Analysis Focus) at the Schar School of Policy and Government. Previously, he was the Country Representative in Malawi of Innovation for Poverty Action, the world's leading provider of Randomized Controlled Trials (RTC) in economic development. A hands-on expert in RCT-based evaluations, a trained econometrician, and a practicing economist, his decade of experience includes field assignments in Indonesia, Malawi, Mozambique, Niger, Philippines, Rwanda, and South Africa. He has been a manager and a staff member in large multilateral institutions such as the World Bank and UNICEF, in research-oriented non-profits such as the International Growth Centre and Khulisa Management Services, and in for-profit development firms including Causal Design and Nathan Consultants. He has published working papers on, among others, food security, teacher performance, tax evasion, and maternal mortality. He has a Master in International Development Policy from Georgetown University, and a B.A. from the College of the Holy Cross.

Mr. Baxter's contributions to this State of the Art Report include Sections 1, 2, 3, 4, and 5, and contribute to his publication requirements as a Public Policy Ph.D. student at George Mason University.

Nathanael J. Bocker

LateralUs, LLC

Nate Bocker is the owner of LateralUs, LLC, a Virginia-based Service-Disabled Veteran Owned Small Business. He holds a Bachelor of Science from American Military University in Environmental Science with a focus Sustainability. He is a veteran of the Marine Corps, the Army, and the Army Reserves. Mr. Bocker served in several capacities, including electronics technician, infantry, and as a power-plant operator. While assigned to the 249th Engineer Battalion (Prime Power), U.S. Army Corps of Engineers, Mr. Bocker began studying vulnerabilities to critical infrastructure and their relationship to community resilience, and the relationships to Homeland Defense. He currently focuses on business workforce development strategies that leverage underutilized demographics to address critical skills gaps in and around Critical Infrastructure Protection.

Mr. Bocker's contributions to this State of the Art Report include Sections 1, 2, 3, 4, and 5.

Jeth Fogg, Ph.D.

North American Aerospace Defense Command/United States Northern Command

Dr. Jeth Fogg is the Engineer Operations and Environmental Chief in the Directorate of Logistics and Engineering at North American Aerospace Defense Command and United States Northern Command with science and technology, environmental, homeland defense, and defense support to civil authorities included in his portfolio. Dr. Fogg has 32 years of civil engineering design, operations, public works, construction management, environmental compliance, hospital life safety, critical infrastructure and homeland security/defense, education and research experience. For the past year, he has been a key member of the More Situational Awareness for Industrial Control Systems team communicating the importance of cyber protection of critical infrastructure for our nation. He holds a B.S., M.E., and Ph.D. in Civil Engineering, a Graduate certificate in Homeland Defense, and Professional Engineer licensure in Colorado and Florida.

Dr. Fogg's contributions to this State of the Art Report include Section 7.

Tyler Goodwin

George Mason University

Tyler Goodwin is currently pursuing his Master in Public Policy Analysis at George Mason University's Schar School of Policy and Government, focusing in technology policy and data science. Prior to attending George Mason, Tyler graduated from the University of Alabama at Birmingham (UAB), where he acquired a B.A. in Political Science and a B.S. in Human Rights Law & Economics. He has held research positions at several organizations since his sophomore year at UAB, including the Institute for Human Rights and his current appointment as a Graduate Research Assistant at George Mason. His policy interests include data privacy, artificial intelligence, algorithmic management, and human rights as they relate to technological progress.

Mr. Goodwin's contributions to this State of the Art Report include Sections 1, 2, 3, 4, and 5, and contribute to his publication requirements as a Master of Public Policy student at George Mason University.

Anura P. Jayasumana, Ph.D.

Colorado State University

Dr. Anura Jayasumana is a Professor in Electrical & Computer Engineering and Computer Science at Colorado State University. He served as a Distinguished Lecturer of the IEEE Communications Society (2014-17) and is currently an ACM Distinguished Lecturer. He received a Ph.D. and M.S. in Electrical Engineering from Michigan State University, and B.Sc. in Electronic and Telecommunications Engineering with First Class Honors from University of Moratuwa, Sri Lanka. His current research interests include Internet of Things, detection of distributed patterns in networks, and mining of network-based data. He has served as a consultant to numerous companies ranging from startups to Fortune 100 companies, and is a member of Phi Kappa Phi, ACM and IEEE.

Dr. Jayasumana's contributions to this State of the Art Report include Section 9.

Dirk Plante

Homeland Defense and Security Information Analysis Center

Dirk Plante is the Deputy Director of the HDIAC where he contributes to the research and development of products across the HDIAC's eight technical focus areas, including critical infrastructure protection. He culminated a 30-year career in the U.S. Army in 2019 as the Chief of Staff and later Chief for Survivability and Effects Analysis at the U.S. Army Nuclear and Countering Weapons of Mass Destruction Agency, Fort Belvoir, VA. Dirk holds a Master in Strategic Studies from the U.S. Army War College, and a Master of Science in Nuclear Engineering from the Air Force Institute of Technology.

Mr. Plante's contributions include Sections 1, 3, 4, and 10, and he served as co-editor for this State of the Art Report.

Steve Redifer

Homeland Defense and Security Information Analysis Center

Steve Redifer is the Director of the HDIAC. His experience includes emergency management, national security affairs, survivability/vulnerability, directed energy weapons, and space systems operations. Mr. Redifer served over 27 years in the U.S. Marine Corps, retiring at the rank of Colonel. During that time, he commanded the Marine Corps' Chemical-Biological Incident Response Force and Region 8 (Central Europe/Balkans), Marine Corps Embassy Security Group. His staff experience includes tours at Headquarters Marine Corps as well as serving in the office of the Director, Operational Test and Evaluation. Mr. Redifer's combat tours include Operation Restore Hope, Mogadishu, Somalia and Operation Iraqi Freedom, Fallujah, Iraq. He holds a M.S. in Applied Physics and a M.S. in Space Systems Operations from the Naval Postgraduate School, a Master of Strategic Studies from the Air War College, and a Bachelor of Aerospace Engineering from Auburn University.

Mr. Redifer's contributions include Sections 1 and 10, and he served as co-editor for this State of the Art Report.

Aleksandra Scalco

Naval Information Warfare Center – Atlantic

Aleksandra Scalco is an engineer with the Naval Information Warfare Center (NIWC) Atlantic. She is working towards a Systems Engineering Ph.D. at Colorado State University. Her research field is cyber resilience for Operational Technology. She earned a Master Degree in Engineering from Iowa State University in 2012, and a Master Degree in Business Administration in 2009. She is a member of the Defense Acquisition Corps in engineering. Ms. Scalco is Defense Acquisition Workforce Improvement Act career certified Level 3 Engineering, Level 1 Science & Technology, and Level 1 Program Management. She holds ITIL Intermediate Certifications. Before joining NIWC Atlantic, Ms. Scalco was a member of the National Security Agency workforce as an Information System Security Designer (ISSD). As an ISSD, she provided technical expertise to clients on cyber assurance to advance the state of cybersecurity.

Ms. Scalco's contributions to this State of the Art Report include Sections 6 and 8, aspects of which are being used to fulfill the requirements for a Systems Engineering Ph.D. at Colorado State University.

Steve Simske, Ph.D.

Colorado State University

Dr. Steven Simske joined Colorado State University in 2018 as a Professor in Systems, Mechanical, and Biomedical Engineering. Before then, he was an HP Fellow and a Research Director in HP Labs. He led HP in research and development in algorithms, multi-media, labels, brand protection, security and secure printing, imaging, 3D printing, analytics, and life sciences. He is a long-time member of the World Economic Forum Global Agenda Councils (2010-2016), leads the Steering Committee for the ACM DocEng Symposium, and is former President of the Imaging Science and Technology professional organization. Dr. Simske has nearly 200 granted U.S. patents and more than 400 professional publications, including the recent books, Meta-Algorithmics and Meta-Analytics. He is an Honorary Professor in Computer Science at the University of Nottingham, UK. Dr. Simske was a payload specialist on a dozen Space Shuttle missions and has designed devices ranging from exercise-responsive pacemakers to impedance tomography systems.

Dr. Simske's contributions to this State of the Art Report include Sections 6 and 8.

Tonya E. Thornton, Ph.D.

George Mason University

Dr. Tonya E. Thornton is the Director of Grants at George Mason University's Schar School of Policy and Government. She is also an Assistant Professor and is the Coordinator for its Emergency Management and Homeland Security graduate certificate. Dr. Thornton is a Co-PI for the Center for Resilient and Sustainable Communities and is an Advisory Council Member for Mason's Institute for a Sustainable Earth. Prior to joining Mason, Dr. Thornton was the Director for the Mississippi Public Safety Data Laboratory where she worked with the Mississippi Highway Patrol in developing computational programs to collect and analyze traffic records data in a timely, accurate, and consistent manner. As a scholar, Dr. Thornton's research portfolio approximates $6 million and has published her efforts in a number of peer review journals, including being a co-editor for the forthcoming Law Enforcement in Emergency Management. Dr. Thornton is an active member of the American Society for Public Administration and serves as a Viewpoint Associate Editor for Public Administration Review.

Dr. Thornton's contributions to this State of the Art Report include Sections 1, 2, 3, 4, and 5.

David Weissman

Colorado State University

David Weissman is a Ph.D. candidate at Colorado State University in the Systems Engineering Department. His current area of research is in cybersecurity solutions for government and business infrastructure advancement. He is currently focused on Internet of Things security, particularly relating the use of deception technology to protect and reduce risk to critical assets. He has worked in advanced technical, business, and financial professional capacities for 25+ years involving both defense and commercial sectors.

Mr. Weissman's contributions to this State of the Art Report include Section 9, aspects of which are being used to fulfill the requirements for a Systems Engineering Ph.D. at Colorado State University.

Executive Summary

The Homeland Defense & Security Information Analysis Center (HDIAC) regularly develops state of the art reports (SOARs) in order to provide a compendium of scientific/technical articles that summarize the most current state of research in topic areas of importance to the Department of Defense (DOD). These SOARs are a means of satisfying user needs for authoritative information directly applicable to their ongoing work.

Critical Infrastructure Protection is one of the HDIAC's eight technical focus areas and was chosen as the subject of our latest state of the art due to its importance to the nation. Critical Infrastructure Protection is composed of National Infrastructure, Physical and Virtual Systems, Cyber Infrastructure, and Continuity of Operations.

The Cybersecurity & Infrastructure Security Agency of the Department of Homeland Security identifies 16 critical infrastructure sectors that are essential to sustaining the economic vitality and high standard of living for Americans: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems, and Water and Wastewater. Their protection must be planned for, which involves the public sector and local, tribal, state, and federal levels of government.

The *National Security Strategy of the United States* asserts that "our fundamental responsibility is to protect the American people, the homeland, and the American way of life… We will protect our critical infrastructure and go after malicious cyber actors." Additionally, nested under the *National Security*

Strategy is the *National Defense Strategy*, and it outlines an operational environment where "every domain is contested – air, land, sea, space, and cyberspace," and emphasizes that the "homeland is no longer a sanctuary." Attacks on our critical infrastructure, both in the physical realm and in cyber space, can cause significant economic disruption, loss of confidence in our civilian institutions, and most importantly injuries to and deaths of countless citizens.

This SOAR reviews the current state of emerging technologies and methodologies relating to the protection of infrastructure and resources critical to national security including public health, financial services, security services (police, military), telecommunications, agriculture, security threats posed from cyber warfare and operational factors and functions, and Continuity of Operations planning. Volume I of this two volume report takes a look at the evolution of our critical infrastructure protective measures, the physical threats to our critical infrastructure, and the role government has in working with the owners of the largely privately-owned infrastructure assets. With our critical infrastructure vulnerable to not only physical but also cyber-attacks, Volume II of this SOAR looks deeper into the cybersecurity threat.

VOLUME I

1

Introduction to Critical Infrastructure Protection

1.1 Identifying and Understanding Critical Infrastructure

Critical Infrastructure (CI) are the essential systems required for the successful functioning of society. They describe "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety [1]." These assets serve as the common thread for public service delivery. Many CI discussions often center on the efficient delivery of government services, relying upon a power grid functioning at full capacity—that they power many of the other systems, such as an operational and expansive communications network, an interconnected and efficient transportation system, and a water and wastewater infrastructure delivering clean and affordable water free of pollution. If one system, particularly the energy system, goes down, it will have both a cascading and compounding impact upon the others. Therefore, the capacity and equity of these systems are pressing problems for all sectors.

Many CI systems are vulnerable, partly due to damage from environmental elements, aging structures, and systems being outpaced by technological advancements they can no longer support. Additionally, with the addition of more users, rising demand will push or exceed existing infrastructure design capacity. The destruction of, or inconsistency in, these systems, assets, and networks, whether physical or virtual, will have a debilitating impact upon economic stability, public health, national security, and any combination thereof for the country.

When examining the term "critical infrastructure," it becomes evident that CI started becoming a part of our American terminology from the mid-1970s to the mid-1980s. Given the rapid advancements

in technology throughout this time period, especially the 'Race to Space' campaign and 'Star Wars' initiative, it was to be expected that CI would become a fixture in the operating world. It was not until the mid-1990s that CI experienced a slight upward trend in daily lexicon, likely as a result of responses to a series of domestic terrorist attacks. It was also during this same time that marked the modern transition of the internet and mentality of "connectivity." Additionally, in May 1998, President Bill Clinton issued a Presidential Decision Directive 63, Critical Infrastructure Protection (CIP) [2]. The directive documented areas of infrastructure that were deemed critical to the national security and economic vitality of the United States and mandated that certain steps were to be made to protect these areas. It tasked relevant government agencies to work on sharing relevant information toward strengthening responses to an attack.

Still, the use and understanding of CI did not begin to peak until the early 2000s, especially as the United States grappled with response to the 9/11 terrorist attacks. The Patriot Act of 2001 defined CI as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [3]."

These trends can be readily seen with Google Ngram Viewer, which permits users the ability to trace the lexicon roots of specific terms (see Figure 1-1).

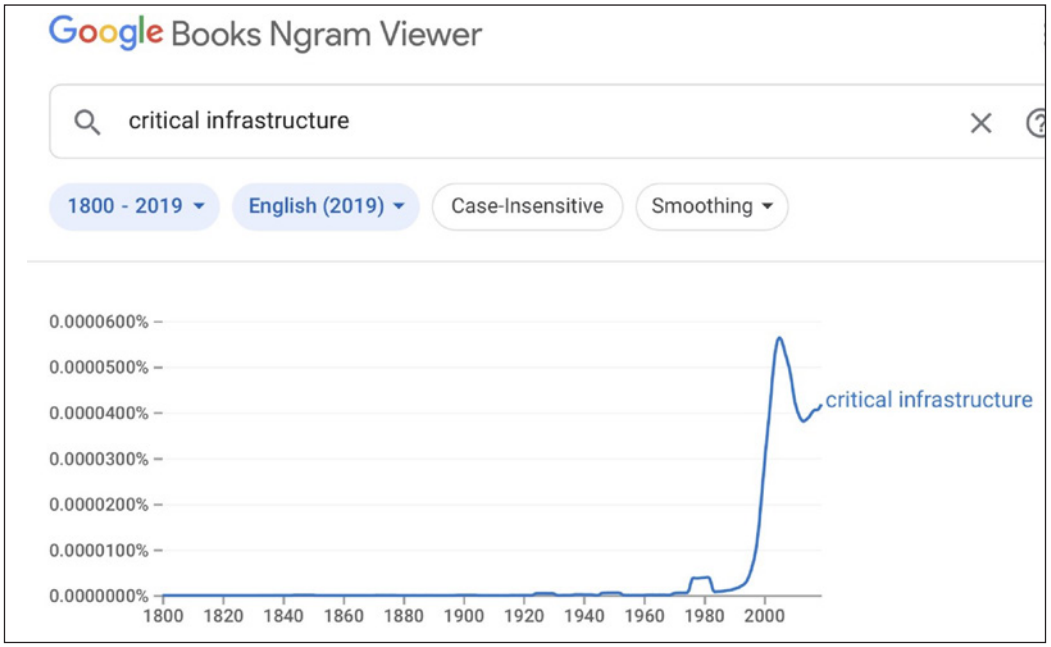

Figure 1-1. Use of the term "Critical Infrastructure." (Source: Authors)

1.2 Defining Aspects of Critical Infrastructure Protection

Following the 9/11 terrorist attacks, the Patriot Act of 2001 reinforced the need for the protection of CI,

an event many consider its defining contribution. This resulted in the establishment of the National Infrastructure Protection Plan (NIPP), a document called for in 2003 by Homeland Security Presidential Directive 7 [4].

The NIPP aims to unify critical infrastructure and key resource protection efforts across the country. It is not considered an actual response plan to be carried out in an attack or emergency situation, but rather as a useful mechanism for strategizing communication, coordination, and cooperation efforts between government and the private sector.

The NIPP was modified in 2013 by Presidential Policy Directive 21, calling for additional measures of resiliency [5]. This revision of the plan established 16 CI sectors. Table 1-1 lists the current 16 CI sectors as outlined in the NIPP.

Table 1-1. Critical Infrastructure Sectors [5].

Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare and Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials, and Waste
Emergency Services	Transportation Systems
Energy	Water and Wastewater Systems

Earlier directives defined the role that the DOD performs as two-fold: As a Federal Department and as the Sector Specific Agency for the Defense Industrial Base [6]:

> *As a Federal department, DoD has both departmental and national responsibilities. Departmental responsibilities include the identification, prioritization, assessment, remediation, and protection of defense critical infrastructure. Additionally, HSPD-7 directs all Federal departments and agencies to work together at a national level to "prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit" critical infrastructure and key resources. DoD and the broader Federal government will work with State and local governments and the private sector to accomplish this objective.*
>
> *As the Sector-Specific Agency for the Defense Industrial Base, DoD has the responsibilities to:*
>
> - *Collaborate with all relevant federal departments and agencies, state and local governments, and the private sector, including key persons and entities in their infrastructure sector;*
> - *Conduct or facilitate vulnerability assessments of the sector;*
> - *Encourage risk-management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources; and*
> - *Support sector-coordinating mechanisms:*
>   - *to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and*

» *to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices*

1.3 Emerging Trends in Critical Infrastructure Policy and Practice

As technologies continue to develop at a rapid pace, the capabilities of our adversaries are being demonstrated at home and abroad. As always, the challenge remains to maintain superiority while continuing to adjust tactics, techniques, and procedures (TTP) to keep pace with the implementation of new technologies. As the threat to CI continues to become increasingly complex, it is essential to remember the fundamental skills that have continued to secure our freedom and the American promise.

> *Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The Nation's critical infrastructure provides the essential services that underpin American society [1].*

The document, *Reducing National Risk,* released in April 2019, adds a perspective to what these actions seek to preserve.

> *National Critical Functions are the functions of government and the private sector produced by infrastructure so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof* [7].

In 2019 the Cybersecurity and Infrastructure Security Agency (CISA) published its risk assessment framework [8], outlining the procedures to assess critical infrastructure. This process, depicted in Figure 1-2, provides a roadmap for agencies to clarify the process for protecting the communities they are responsible for.

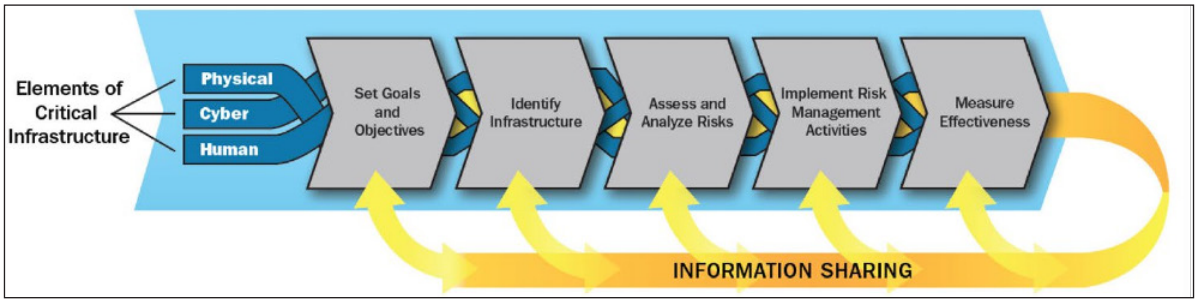

Figure 1-2. U.S. Critical Infrastructure Risk Management Framework [8].

National Institute of Standards and Technology (NIST) Special Publication directive 800-171 provides guidance on cybersecurity for nonfederal organizations supporting federal activity [9]. The guidance applies to controlled unclassified information (CUI) systems that do not already have specific laws or regulations enforcing the security of data. The DOD Cybersecurity Maturity Model Certification,

which is still under review for modification, lays out the framework for those organizations working within the DOD ecosystem. While recognizing the need for vigilance and security, there has been pushback from the private organizations working with DOD, claiming that these requirements will make it harder for them to remain competitive and profitable.

1.4 Nexus of Critical Infrastructure Systems

To fully understand CIP, it is necessary to see not only the vulnerabilities to each sector, but also to understand the interrelated and cascading functions of CI sectors within the ecosystem. Examining how disruptions in one sector affect other sectors demonstrates the cascading relationships across the system of systems. A risk analysis approach can be used to clarify the confusion of a simple assessment of all sectors and can assist with identifying areas that are more susceptible to vulnerability.

Similarly, showing accumulative risk and vulnerability allows for the identification of contributors to the vulnerability of other sectors. For example, a failure under the energy sector would likely have a cascading effect across all areas of critical infrastructure, but it will be immediate. Vulnerabilities to public health may also affect all sectors, but over a much longer period of time. Vulnerabilities to communications may not be as catastrophic as a disaster at nuclear facilities, but the effects may be more widespread geographically. These and vulnerabilities resulting from interelated and interconnected CI will be discussed throughout this report.

2

Threats to and Vulnerabilities of Critical Infrastructure

2.1 Introduction to Threats and Vulnerabilities

The CISA risk management framework (See Section 1, Figure 1-2) recognizes three elements from which threats appear: Physical, Cyber, and Human. While risks do not always remain within a single category, identifying these allows for a more detailed understanding in order to manage risks.

Physical threats are those that disrupt the actual mechanics of the sector functions. Power outages, water main breaks, server crashes, and even construction on the interstate to repair roads are physical disruptions. The aging and decay of systems are expected and planned for, but there are times when parts of these systems fail suddenly. A natural weather event may cause damage to a system, which may further disrupt other systems because of the interwoven nature of CI. As technology advances in capability, many physical threats can be identified and mitigated. Meteorology, predictive maintenance analytics, and automated security can aide in reducing response times to physical threats, but also contribute to a more interdependent ecosystem.

As CI systems become more connected, cyber threats become more prolific. These threats occur when the connectivity of these systems provides the means for failure, often by human effort. An automated process that relies on connectivity can be targeted and disrupted by attacking the network itself. Also, accidental disruptions may happen due to unintentional causes. For example, the failure of a firmware update may cripple a process that supports a critical function, such as wastewater treatment or cellular communications.

The most common cause of disruption, intentional and otherwise, is human. Insider threats, bad actors, and human error contribute to the majority of disruptions, and it is often a root cause of cascading

failure. Nation-state and transnational actors, radicalized individuals, and other groups target CI, often using the human element itself as a means to gain access. Phishing scams, manipulation, and human error provide adequate avenues with which to attack critical infrastructure from the outside. These threats can be the result of any number of influences, from political, to social, to economic, to ideological.

As systems become increasingly more complex, the likelihood of human error also increases. The ability of the human mind to maintain awareness of complex systems has limitations. The ability to multitask or to follow subtle, unexpected changes in an environment is partially mitigated through process and procedure, but these are only effective to a degree. Automation of these processes enhances awareness, but without careful prioritization, this approach can be equally overwhelming.

A mirrored approach to risk mitigation is to consider the targeting aspect, especially concerning nation-state and transnational actors. Just as with the risk vectors, the potential targets can also be categorized as physical, cyber, and human. By considering threats through the lens of this expanded model, threats can be analyzed to examine how these systems may be affected. While the majority of focus remains on physical and cyber infrastructure, the addition of the human element expands the focus to consider attacks directed at undermining political process, social structure, governmental roles, etc. [10].

This approach highlights the need for concern regarding the role of information warfare in its current and future forms. While traditionally used as a force multiplier for kinetic warfare, more advanced forms of information (and disinformation/ misinformation) warfare are beginning to be used on their own. The cognitive domain of warfare specifically targets human populations and how they perceive their environment, which exacerbates real or perceived polarizing dialogue. The 2016 and 2018 elections in the United States and as a precursor, the 2014 Ukrainian elections, demonstrated Russia's willingness to leverage information warfare as a primary strategic advantage [11].

The recent shift in focus towards cyber elements of CIP highlights the recognition from both the public and the private sectors of the importance of remaining aware of rapid creation, adoption, and integration of new technologies. As technology continues to change at a rapid pace, it is necessary for policymakers to remain aware of these changes.

Challenges to privacy policies will require finding ways to educate and inform those serving in official capacities with responsibility for CI systems, as well as the general public. The industry-accepted Cyber Kill Chain (developed by Lockheed Martin) and other hybrid models to account for the steps taken to disrupt and defeat systems are threat focused, however it may be necessary to develop a systems-based approach to identifying vulnerabilities to systems, and developing security measures focused on the system versus the threat. By identifying all potential vectors of vulnerability, including cyber, insider threats, physical (including manmade and natural disasters, etc.) the approach would assist policy makers, both public and private, to identify areas lacking focus and clarity.

As much of policy writing and implementation still follows an iterative approach, it is outpaced by vulnerabilities, leaving increasingly large gaps between mitigation and risk. The increased capabilities of technology might be leveraged to assist with decision-making, by modeling the built environment, and examining how the results of these decisions might affect communities.

For example, the construction industry has been using modeling and simulation for energy efficiency and sustainability for some time now. The integration of building information modeling (BIM) into design practices has allowed engineers to make informed decisions about everything from building location to material choice. A similar approach might be used to simulate critical infrastructure and supply chain management as a proactive approach to planning for disasters. The use of modeling for water use, based on data from historical rainfall allows for resource use and planning, and contributes to infrastructure protection by identifying where criticalities lie in these systems.

And in a final example, modeling and simulation in healthcare has allowed for more informed decision making from both consumers and policy makers but is still not fully adopted. Part of the challenge is teaching those who are not familiar with new technologies how to integrate these technologies into their organizations. Healthcare in particular will be challenging, since there is a need for evidence based on clinical trials, but the modeling can still support these trials to assist with (and reciprocate verification of) validation [12][13].

2.2 Changing Security Challenges

When looking for the root cause of system disruption and failure, it is essential to consider the role that CI plays in gray zone warfare. The gray zone is conflict that does not cross the threshold of warfare, which may be due to ambiguity of international law, complexity of actions and attribution, and/or because the impact of such activities do not justify a measured and operational response [14]. Conventional warfare is economically exhausting and hybrid warfare may be able to accomplish the same ends that traditional warfare sought to bring about. Disruption of CI has long been used to aid conventional warfare, but the shift in global climate has made armed conflict less attractive. Achieving dominance over an adversary without firing a single shot may be increasingly possible and could lead to new ideas about what constitutes an act of war.

As sectors become more connected to information technology (IT), operational technology (OT), and internet of things (IoT) systems, the CIP challenges have compounded. While these sectors all have their own specific threats to deal with, the addition of connectivity to these systems adds to the vulnerability. It is not simply that there is now a cyber component, but that existing issues are compounded by the addition of connectivity. The use of social media, IoT devices, and systems monitoring energy consumption, all contribute to vulnerabilities by creating avenues of attack within the CI ecosystem.

A hybrid collaborative approach will likely be needed to address challenges. It is unrealistic to assume that any single person can address all threats as evidenced by the large-scale growth in public-private partnerships are required at larger scale. By focusing on building cross-functional teams around critical infrastructure sectors, including those familiar with systems thinking, the prevention and responses will model the threat environment. The disconnected systems, themselves, are complex, but when looked at as a system of systems, it is easy to become lost without a team that understands the interrelationships. When these systems are attacked or are subjected to a natural event, a failure in one can rapidly cascade into other areas.

Another contributing factor to these risks is the increasing complexity of the CI sectors themselves, and cross-communication between siloed industries. For example, an attack on the energy sector may appear as a fault in the protection systems, such as a ground fault. Without communication between cyber professionals and electrical experts, it may take weeks to discover that the apparent fault was not from the physical system but a cyberattack on supervisory control and data acquisition (SCADA) systems. Similarly, the integration of wireless technology to reduce infrastructure and increase connectivity can be targeted for accessing systems.

The human terrain has also shifted, with the increasing role of social media, not only as a personal tool but as a business tool, is an area of concern. Many cyberattacks begin with social engineering, and the increased reliance on social media for workforce recruiting, advertising, and public awareness campaigns provide avenues of attack. While operational security (OPSEC) is a familiar topic within the Armed Forces, a private business may not be aware of how their “reason to celebrate a new contract” or

a "picture of new equipment" might be just the information needed to exploit a vulnerability.

In recent years, there has also been an uptick in hardware level backdoors, and circuit designs that can provide access to devices. There are techniques to examine chip circuitry for side-channel emissions, and there have been discoveries of these factory-installed backdoors in chips [15]. With many companies outsourcing their manufacturing to other countries, there is the possibility that there is malicious intent behind these compromised chips. These built-compromised devices provide an open route with which an adversary can load software to give unwanted access to systems, or simply leak information to unknown actors. This level of sophistication is not necessarily a tactic reserved to a nation-state but could also be used for business espionage. By collecting data from any source that uses the compromised equipment, it would not be unrealistic for the collector to broker data to anyone willing to pay for it.

The use of global positioning system (GPS) information from cell phones can also reveal sensitive information, as demonstrated by the use of exercise apps to map troop movements. DOD banned the use of these apps in forward-operating areas precisely because of this vulnerability. This vulnerability clearly becomes a more significant concern when the country of origin for cell phone applications and hardware are considered. The proliferation of GPS data allows for tracking of personnel, identifies commonly used routes, and builds a profile of where and when facilities are accessed or left vacant [16] [17].

The use of apps, many of which have been designed to generate and drive user engagement, have also become increasingly invasive. The proliferation of low-level personal data, like passwords, photos with GPS tagging, or emails and files, is not the only concern. With increasing processor speed on smartphones, it has become the norm to include haptic feedback and biometrics for device security. With compromised software and hardware, this data can be combined to create considerably more subtle attacks. Historically, breaches of data security were a primary concern, but this higher-level proliferation encompasses fingerprints, eye-movement patterns, color preferences, and behavior patterns. These minute details can be used to create a digital persona of a user. The use of these personas can then be used to generate targeted manipulation of human psychology and physiology.

The saturated built Wi-Fi environment of the future increases risk of privacy loss. With the integration of 5G technology, a recent paper published through Massachusetts Institute of Technology demonstrated the ability to use Wi-Fi to see through walls and identify biological characteristics for individual identity. This presents several problems for DOD and other government facilities, where Wi-Fi is in use. Recent developments in both software and an understanding of radio signal have allowed for software recognition of individuals through walls, using Wi-Fi antennas and routers. The electromagnetic saturation of the built environment becomes even more concerning with the realization that 5G will increase the number of connected devices from about 2,000 per .38 square miles to over 1M for the same area.

The intersection of a hyperconnected environment and artificial intelligence (AI) for rapid data aggregation and use creates the conditions for even more advanced gray zone conflicts. Battles may be fought by land, sea, air, or space, but the digital realm will cross all domain [18][19].

2.3 Evolving Role of Information Technology

Information Technology and the protection of data is becoming increasingly complex. The data itself is a recording of every aspect of connected systems. As information about system behavior and interaction is collected and stored, often remotely in data centers, the risk of proliferation increases.

As the drive to connect devices for smart systems continues, the data from these systems and sensors paint a clear picture of how our systems work. The data not only show peak use times for not only water and energy, arrival times for shipments, patterns in finance, upticks in manufacturing but also the human patterns of behavior that drive these events. The data give those with access information that can be used against citizens and infrastructure.

Future attacks against CI will be both increasingly complex and subtle. Access to this data can facilitate cyberattacks, and an adversary can manipulate built environments to cause disruption and harm. Targeted attacks on a heating, ventilation, and air conditioning (HVAC) system, for example, do not seem severe on the surface, but human reactions to subtle shifts in the environment can be disruptive to workflow. If this were to occur, say, in the office environment of a federal building, the shift in temperature might be used to disrupt or distract from a coordinated attack in another area. If the environment requires certain parameters, such as for food storage, such an attack could not only spoil food but lead to illness or even death.

It is becoming ever cheaper to attain the means to conduct these attacks, and their scale can range from minor to massive. The level of skill required to perform a cyberattack is lowering as technology advances, furthering the risk of a cyberattack on CI. Cyber terrorism is a problem that threatens several areas of CI. Any organization that deals with electronic databases is vulnerable to a cyberattack. If one sector of CI falls victim to one of these attacks, then the stabilization of CI as a whole is jeopardized due to the interlocking facets of CI.

On February 18, 2020, the Department of Homeland Security (DHS) confirmed a ransomware attack had targeted CI at a U.S. natural gas compression facility. DHS announced a "cyber threat actor used a spear-phishing link to obtain initial access to the organization's information technology network before pivoting to its operational network [20]." DHS went on to say that the natural gas facility was not equipped to handle a cyberattack. As a result, the facility was forced to shut down for two full days, though the attack "did not impact any programmable logic controllers and at no point did the victim lose control of operations [20]." In May of the same year, the National Security Agency confirmed Russian hackers used a computer virus that allows them to remotely control U.S. servers. Additionally, U.S. officials claim Chinese hackers tried to steal data about a COVID-19 vaccine on behalf of the Chinese government [21].

According to the Center for Preventative Action's 2020 Preventative Priorities Survey, a cyberattack on U.S. critical infrastructure is the 'top tier' priority. As tensions with Iran and China escalate following the relations-damaging actions over the past year, Iran's ICT Minister Mohammad Javad Azari Jahromi announced, "The Islamic Republic of Iran and China are standing in a united front to confront U.S. unilateralism and hegemony in the field of IT [22]." And although China's cyber power is not near as advanced as the United States, the Chinese government is "using cyber power to rise and ultimately win global dominance [23]."

Claroty, a leader in cybersecurity, released a report on the current state of cybersecurity worldwide in March 2020 [24]. Their research indicates that "74 percent of IT security professionals globally are more concerned about a cyberattack on CI than an enterprise data breach." The report also found "more than half of the industry practitioners in the United States (51 percent) believe that today's industrial networks are not properly safeguarded and need more protection, while another 55 percent believe that U.S. critical infrastructure is vulnerable to a cyberattack." Furthermore, 63 percent of IT professionals in the United States reported they "expect a major cyberattack to be successfully carried out on national infrastructure within the next five years," while 10 percent reported they believe the United States will "never see one, despite ample evidence of attacks targeting energy and other related sectors."

Cyberattacks are not limited to accessing a database or shutting down a power grid – attacks are ever evolving alongside technology. Some attacks are based in human interaction to persuade people, typically employees, to break standard security protocols (social engineering). Social engineering is an attack that depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information. Today, social engineering is recognized as one of the greatest security threats facing organizations [25]. This method of attack is much less technical than one that remotely breaks into a software, but equally as threatening. Phishing is a means of social engineering and happens more frequently at heavily protected sectors of CI, such as nuclear power plants and power grids. By sending targeted, malicious emails, engineers who work in such facilities are at risk of compromising their entire facility by simply opening an attachment [26][27][28].

The biggest threat to our CI in terms of social engineering is the element of trust; that one's individual nature to trust is what makes them vulnerable. "Even those who believe that they are not trusting by nature, with the right story, speech, voice, and body language, social engineers can and do find their way [29]." Pollack et al. conclude by identifying emails as the primary gateway for malicious attacks on CI and call for organizations to "adapt to the advanced threat systems [29]."

2.4 The Strain of System Overload

The challenge, as more technology becomes connected presents two issues: the complexity of the systems themselves, and the human element. The first requires subject matter experts who understand the systems they work on and around, and the second requires "the spotter" who sees how these systems interrelate. It is unrealistic to expect any single operator to be able to keep up with the complexity of current and future systems. Much like studying natural environments, a multidisciplined cooperative approach is necessary.

The cascading, compounding, and co-occurring effects within the complex ecosystem of CI indicates that a siloed approach does not support security efforts. For both proactive and reactive response to CIP, it is necessary to understand what connections there are between sectors of infrastructure, and how these sectors interact. The complexity of the system itself is a contributing factor to how infrastructure may suffer failure.

If the connected systems are not built and maintained with overlapping influence of each other, a minor failure in one sector may result in catastrophic failure in others. Likewise, multiple minor disruptions across multiple sectors may feed off each other, creating a larger overall disruption.

On the surface, this system seems simple enough, but consider also the supply chain of fuel involved, or the communication system that carries signals for metering, switching, etc. [30]. The system itself supports another sector, say wastewater treatment or oil refinement. A disruption in any of these systems would influence how both contributing and follow-on systems function.

Likewise, by considering the human element of these systems and how they can be used to target public sentiment and social structure, the need for both better strategies and better means of protection becomes apparent. The attacks on CI are not new to warfare, but as the capabilities of gray zone warfare continue to develop, it becomes increasingly important to understand the threats to and vulnerabilities of CI. For example, in an electrical system, components are always used with surge capacity in mind. The typical load on the system should not be the maximum load the system is capable of, to allow for an increase in demand. By building flexibility into the circuit, the risk of failure from overload can be significantly reduced. If, however, there are normal conditions when the draw against the system suddenly exceeds the capacity of a single component, the system will fail.

2.5 State of the Art

Advancements in new technologies, such as AI, predictive analytics, and big data utilization, have greatly benefitted and strengthened CIP efforts. Government agencies in the United States are using these technologies in effective and innovative ways for natural disaster response, improving safety protocols, maximizing military strategies, and many other areas. As technology advances, it becomes more integrated into the lives of everyday citizens. The same can be said about technology's relationship with CI. Trends show specifically in the past decade, technology has become increasingly vital to CI and CI support.

Today, AI capabilities allow for sound predictions that pertain to CIP. It was always possible to make these predictions, however AI has removed the difficulty of computing the probabilities longhand. For example, it is now possible to predict how many residents in a given area will be without power following a natural disaster, such as a hurricane or tornado, because there is a significant amount of data logged during past natural disasters in the same area or ones similar to it. It could take a human a number of days, weeks, months, or even years to make such statistically sound predictions, but that is no longer the case due to AI. Storing large amounts of data to be analyzed in order to identify trends and patterns is what is known as big data. While it is nearly impossible for a human to analyze big data, AI is capable of analyzing it in minutes, sometimes even seconds.

By adjusting the approach to these challenges to focus on CI as a system of systems, it is possible to build both secure and resilient systems. The continual advancement of capabilities that aid Information Warfare and Cognitive Domain Warfare will need special attention [31].

In addition to AI, microgrids are beginning to play a large role in CIP. The Department of Energy (DOE) defines a microgrid as a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously. Autonomy is what makes a microgrid vital for CI; working independently is what allows CI to use locally produced energy after a natural disaster or some other disruption to the primary power grid. If an area experiences a blackout, microgrids can utilize local energy to begin the restoration process. Resiliency is the key benefit of microgrids.

Microgrids are able to enhance the reliability and durability of a power grid and are already considered to be the future of power systems. As cyberattacks become more sophisticated while also requiring less skill to utilize, microgrids are more likely to be targeted. Decentralization is the solution to this problem, because it diminishes the importance of any one microgrid. Another advantage of microgrids is the concept of "mutual suspicion" in network design. "Through mutual suspicion, peers protect themselves and their neighbors by recognizing that communication channels and even peers may be compromised. While the monolithic legacy grid doubtless includes examples of these defensive strategies, safety and correctness would require that mutual suspicion be an integral aspect of a functional microgrid architecture, rather than an afterthought [32]."

Similarly, edge computing pushes the computational aspects of cloud computing to the user or device's physical location, decreasing the bandwidth requirements and reducing latency and jitteriness [27][33][34]. This computational power can also be used to address the resources needed for complex access security algorithms, increasing the security of IoT devices and systems. Tertiary benefits to security are bandwidth usage and latency reduction, allowing for anomalies to be rapidly identified with predetermined response protocols. Research into 5G and 5G networks suggest that channel allocation can be performed by deep learning algorithms, allowing for precise and condensed usage of spectrum [35]. Other AI solutions include anomaly and latency detection and other security tactics.

Further understanding of the human terrain will be vital to counter these efforts. Beyond simple behavioral science, there will need to be a comprehensive effort to define cognitive aspects of both the

individual and social terrains. Narrative warfare, memetics, biohacking, and other forms of information warfare and perception manipulation are already being used by nation-state and transnational actors. The increasing sophistication of deep fakes and digital manipulation will cause a decrease in trust of traditional centers of influence, and as a macro or metawarfare strategy, will seek to cause degradation in social structures. The follow-on chaos and disruption can serve as a diversion from other tactics, or may be the desired end state.

3

Role of Federal Government in Critical Infrastructure Protection

3.1 Introduction to Role of Federal Government

The United States faces many challenges in protecting its CI, including the nation's vast size, geographic layout, layers of governmental regulations, and the age of various parts of the infrastructure. Making protection additionally difficult is that a large number of these CIs are owned by multinational corporations. Private entities own the vast majority of CI. These entities not only provide services to citizens and other private entities, but they also provide services to agencies and departments across the federal government, enabling these agencies to fulfill their obligations to the American people. The mandate to the federal government is to ensure these services are protected and secured. Increasingly, this mission is supported through public-private partnership (PPP) initiatives, such as InfraGuard (the FBI's PPP taskforce), Protected Critical Infrastructure Information (PCII) (CISA's PPP assessment platform), among others. These programs work to share information across the PPP boundaries, with a focus on assessing and providing feedback on vulnerabilities and disseminating information about cross-cutting threats.

Critical infrastructure is made up of several, independent actors that may influence any and perhaps even all other areas with even the smallest action; as aforementioned, a system of systems. When performing risk analysis or trying to maximize output, it is difficult to fully understand how one decision may affect other sectors of CI. If you were to map out the effects any one decision could have on CI, the resulting map would look chaotic. That is where AI comes in – to read the chaos and present conclusions in a way that is easier to understand, thus allowing for the agencies in charge of CI to act

more swiftly and effectively. By using predictive analytics and statistical learning, two of the most powerful tools in the AI-arsenal, not only is identifying vulnerabilities within a sector easier, but so too is identifying the potential cascading effects adjusting that vulnerability or other actions may cause, which allows for CIP to be maximized.

The Patriot Act of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [3]." These systems are prioritized further, across the 16 sectors, with four sectors identified as lifelines, which the degradation of, would cascade into other sectors with severe consequences. Per the Government Accountability Office (GAO), Water, Energy, Communications, and Transportation Sectors are major systems for the United States, and interrupting the continuity of any one of these systems could result in catastrophic property damage, human loss of life, and substantial economic losses [36]. Reliable operations of the four lifeline sectors – transportation, water, energy, and communications – are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors. For example, energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors; in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication) [37]. Figure 3-1 shows the connectedness of the four designated lifeline sectors with all other CI.

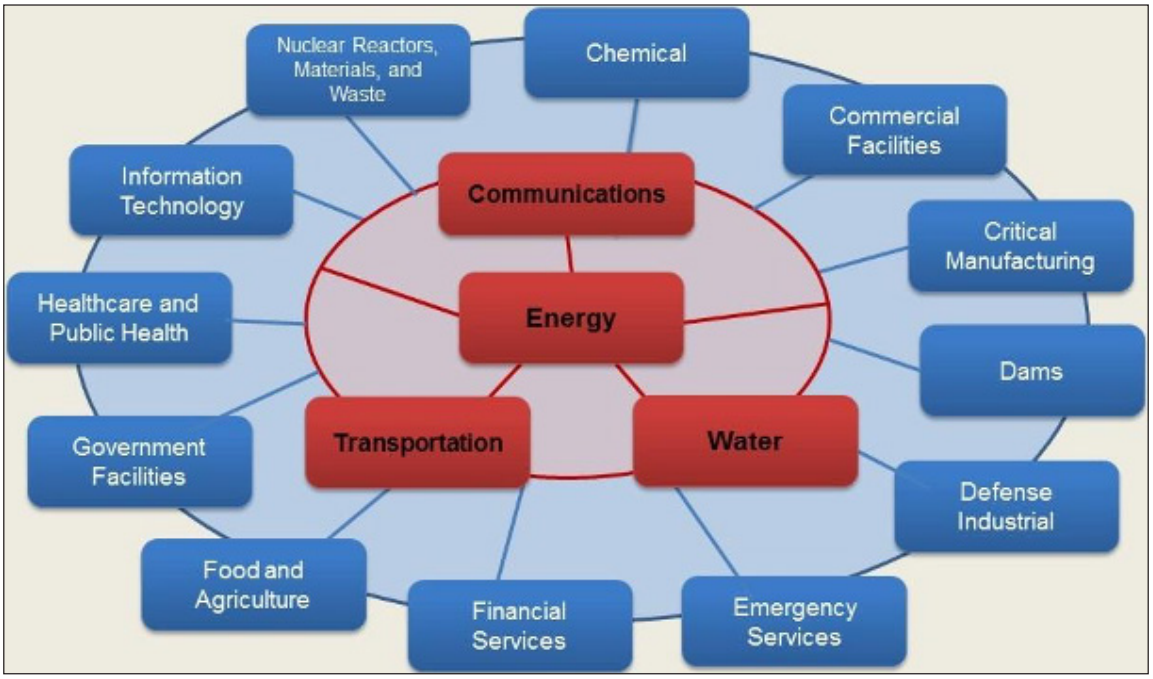

Figure 3-1. The four designated lifeline functions and their affect across other sections (Source: Authors).

3.1.1 Water

The Water and Wastewater Infrastructure Sector, under the jurisdiction of the Environmental Protection Agency (EPA) and in cooperation with public and private stakeholders, focuses on ensuring that this fundamental human need is available and safe for the population of the United States. The goals of the Water and Wastewater Systems Sector-Specific Plan (SSP) highlight Human Health, System Resilience, and Recognition of Risk as the primary focus of these effort [38].

While EPA holds jurisdiction over this sector, the U.S. Army Corps of Engineers (USACE) also plays a large role in keeping the water flowing. Their primary responsibility is to ensure that the commercial water infrastructure remains in working order and that it is protected from threats. America's Water Infrastructure Act of 2018 provided an additional $3.8B in funding for additional new infrastructure projects [39], and the 2019 Fiscal Budget appropriated an additional $7B towards the same goal. This much-needed boost is directed to improving the resilience of water systems.

DOD's primary interaction with EPA is through USACE coordination. USACE is responsible for maintaining the nation's commercial waterways and operates the dams and locks that facilitate commerce on inland waterways. A number of drinking water systems use dam reservoirs as their primary water sources, thus dam safety and protection is a critical issue for the Water and Wastewater Sector. Some employees of the USACE Engineering Research and Development Center also sit on the EPA's National Homeland Security Research Center (NHSRC) Distribution System Research Consortium (DSRC). Military facilities with their own drinking water and wastewater systems are regulated under the Safe Drinking Water Act (SDWA) and Clean Water Act (CWA) and where applicable, must complete and submit vulnerability assessments to EPA [40].

3.1.2 Communications

The Communications Sector focuses on the protection of physical and logical health of communication systems, providing support services to enhance resilience, and to coordinate preparedness efforts between stakeholders. Managed by DHS, the focus of the Communications Sector is on broadcast, cable, satellite, wireless, and wireline infrastructure. The Communications SSP identifies the risks to communication infrastructure and lays out the goals to maintain present and future security [41][42].

Disruptions to assets in the Communications Sector must be avoided whenever possible. When a manmade or natural disaster strikes, the CI assets in the Communications Sector are vital for broadcasting emergency alert messages to keep the public informed. Risks to the sector include vulnerabilities to the supply chain that can impact the availability of new and replacement hardware and software; and cybersecurity threats that can impact the proper functioning of communications equipment across the sector. The federal government engages with industry in a number of public-private advisory and operational forums to ensure proper planning, implementing, and execution of sector-wide resilience for communications infrastructure.

3.1.3 Transportation Systems

The Transportation Systems Sector covers aviation, maritime, freight rail, highways, pipeline, postal/shipping, and mass transit. The focus of the Transportation Systems SSP is to manage security risks, employ sector capabilities to support resilience, and implement processes to share information about risks and threats to the infrastructure [43].

The Transportations Systems Sector is co-managed by the Departments of Homeland Security and Transportation, with DHS delegating its responsibilities to two subordinate organizations, the Transportation Security Administration and the U.S. Coast Guard. The Transportation Systems Sector is an example of the vast physical breadth a CI sector can cover, and how sensitive to risks it is with several interdependent sectors such as Chemical, Communications, Critical Manufacturing, Dams, and Water and Wastewater Systems [43].

Examples of the assets in the sector include more than 4 million miles of roadway, 600,000 bridges, hundreds of tunnels, 2.5 million miles of pipelines, 25,000 miles of navigable waterways, hundreds of ports, 140,000 miles of rail track, and hundreds of commercial airports [43]. Each of these assets is susceptible to manmade and natural risks that could have cascading impacts affecting other CI sectors if not properly assessed for risk reduction and mitigation.

3.1.4 Energy

A nation's energy system supports the essential functioning of governance and society. This is the common thread that touches and weaves through our lives. The Energy Sector is managed by DOE, with support from DHS, and is focused on securing the electrical grid, electrical power production, and oil and gas infrastructure [44].

Energy systems influence our lives in every way, from access to electricity and transportation, cultivation of food and use of water, exploitation of natural resources, impacts on human health and environment, and economic and national security. To be competitive in an interdisciplinary environment impacted by these areas requires a comprehensive understanding of the politics of global energy, the economics of energy supply and demand, the resiliency and adaptability of energy infrastructure and technology, and the social and environmental impacts of energy.

Lastly, the COVID-19 pandemic highlights myriad threats, vulnerabilities, and opportunities within the energy sector some of which are truly unprecedented. For instance, with oil prices entering negative territory, rentier hydrocarbon nations may soon risk becoming "failed states" creating social instability. Similarly, a new appreciation for resiliency may precipitate a more distributed energy grid, loosely connected, but centrally managed. Although the full impact is still very uncertain there is reason to believe disruptive changes will emerge.

3.1.5 Other Sectors

Beyond these core elements, CI supports the Federal Government, including DOD missions, in other ways. From ship-building to support the Navy's efforts or rail transportation to move Army and Marine Corps equipment between installations for training exercises to financial services to ensure contract payments and food supplies to feed service members and their families, the ecosystem of infrastructure ensures that DOD can fulfill its mission to defend the homeland.

While only one sector of CI has DOD as the Sector Specific Agency (SSA), the Defense Industrial Base (DIB), all threats from external sources fall under the purview of DOD. When threats originate from a nation-state or transnational actors, the DOD is the responsible agency for coordinating the defense of the affected assets.

The DIB Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The DIB partnership consists of Department

of Defense components, more than 100,000 DIB companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities. The DIB companies include domestic and foreign entities, with production assets located in many countries. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The DIB Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements. These commercial infrastructure assets are addressed by other SSAs.

Because DOD also supports SSAs when it is the most capable to address a specific threat, its role may appear ambiguous at times. For example, the Transportation Systems Sector SSA is the Department of Transportation. If a disruption in this sector resulted in a chemical spill or similar incident, DOD has the training, equipment, and personnel who are able to perform large scale HAZMAT operations. Many of these overlapping roles are defined under FEMA's ESF framework for National Response [45]. Table 3-1 lists the CI sectors along with the agencies of the Federal government designated in PPD-21 with specific responsibilities by leveraging their particular knowledge and expertise [46].

3.2 Homeland Defense

The support that DOD is allowed to provide, framed within the confines of the Posse Comitatus Act from 1878, is limited to threats originating outside the United States, threats against the DIB sector, or situations where civilian agencies do not have the capacity or experience to deal with situations adequately.

DOD plays a vital role in all three missions involving the homeland — homeland defense (HD), homeland security (HS), and defense support of civil authorities (DSCA). The key difference between the three missions is that DOD is responsible for the federal response to HD; DOD is in support of other federal agencies' HS responsibilities; and DOD conducts DSCA operations in support of another primary agency supporting a state, local, territorial, or tribal response. DOD works with the DHS and other United States Government (USG) departments and agencies to accomplish these missions [47].

The combatant command that is responsible for coordinating all HD efforts is U.S. Northern Command (USNORTHCOM). It was established in 2002, and is located at Peterson Air Force Base, Colorado. USNORTHCOM is structured to align all DOD HD assets under a single command, with components of all branches of the DOD represented. USNORTHCOM subordinate units are U.S. Special Operations Command, North; U.S. Marine Corps Forces Northern Command; U.S. Fleet Forces Command/U.S. Navy North; Air Forces Northern; U.S. Army North; Joint Task Force North; Joint Task Force Civil Support; Alaskan Command; and Joint Force Headquarters National Capital Region.

Table 3-1. Sector Specific Agencies [46].

Critical Infrastructure Sector	Sector Specific Agency
Chemical Sector	Department of Homeland Security
Commercial Facilities Sector	
Communications Sector	
Critical Manufacturing Sector	
Dams Sector	
Emergency Services Sector	
Information Technology Sector	
Nuclear Reactors, Materials, and Waste Sector	
Defense Industrial Base Sector	Department of Defense
Energy Sector	Department of Energy
Financial Services Sector	Department of the Treasury
Food and Agriculture Sector	Department of Agriculture and Department of Health and Human Services
Healthcare and Public Health Sector	Department of Health and Human Services
Transportation Systems Sector	Department of Homeland Security and Department of Transportation
Government Facilities Sector	Department of Homeland Security and General Services Administration
Water and Wastewater Systems Sector	Environmental Protection Agency

The challenge to DOD when dealing with the private sector is finding the correct incentives to foster a proactive approach to protect assets. This challenge is twofold: financial and cultural. The 2018 Report on Manufacturing and the DIB identified instability in the acquisition process as a significant contributor to companies leaving the DOD ecosystem [48]. The financial difficulty in keeping abreast of the process and the effect that disruptions to funding have on the private industry is a deterrent to proactive involvement.

The cultural differences between government agencies and private sector business compound the problem. While private sector business does work to address threats, the culture within these entities is rarely focused on threat detection and mitigation. Communication from DOD, and other security-focused agencies, may sound alarmist to those unfamiliar with the context in which DOD works in. The intelligence gathering efforts of DOD imply that not everything can be openly shared. Public dissemination of intelligence briefings is hampered by the inherent differences between federal agencies and civilian entities, given the nature of the subject material. Streamlining the process to

clear information further, will play a vital role in efforts towards bridging these gaps to correct existing and future vulnerabilities facing CIP. Without clear communications guidelines and cooperative information sharing, the PPP efforts will be hampered.

AI now has a strong presence in military operations. It has the capability to destabilize the balance of power in strategic operations. Sharikov argues, "With the advent of [advanced AI], more targets have become available for computer hacking, meaning that critical infrastructure – banking systems, airport flight tracking, hospital records, the programs that run the nation's nuclear power reactors – can be vulnerable [49]." The ability to conduct such attacks poses dangerous implications for CIP. For AI to protect against a cyberattack from another AI-entity innovative programmingis required. Sharikov continues to say, "the defense must be self-learning, so it can learn the specifics of an offensive technology [49]." Sharikov concludes his paper by acknowledging the importance of military AI research and protocol remaining in total control by the government; this, he argues, will preclude any unauthorized use and attacks.

3.3 Emergency Management

Anyone who has witnessed a natural disaster unfold in recent years is likely aware that the federal government plays a role in responding to these events.

The National Response Framework (NRF) and subsequent Emergency Support Functions (ESFs) lay out the procedures for responding to disasters, identify the organizations with responsibility to each sector, and outline the process for deploying federal support. Within this framework is the annex that describes the process for CI-related events.

The ESF roadmap explains which federal agencies hold responsibilities under a DHS deployment, and the circular relationship that DOD has with this framework is summarized in Appendix B. It states, "When requested, and upon approval of the Secretary of Defense, DOD provides DSCA during domestic incidents. In the context of the NRF, DOD is considered a support agency for all ESFs. DOD is the SSA for the DIB sector, which may have links to many of the ESFs."

Joint Publication 3-28, Defense Support of Civil Authorities, updated in 2018, highlights DOD roles and responsibilities in support of the NRF and the broader ESF functions. In its Overview, it states:

> *Defense support of civil authorities (DSCA) is support provided by federal military forces; Department of Defense (DOD) civilians; DOD contract personnel; and DOD component assets, to include National Guard (NG) forces (when the Secretary of Defense [SecDef], in coordination with the governors of the affected states, elects and requests to use and fund those forces in Title 32, United States Code [USC], status), in response to a request for assistance (RFA) from civil authorities for domestic emergencies, cyberspace incident response, law enforcement support, and other domestic activities or from qualifying entities for special events. DSCA includes support to prepare, prevent, protect, respond, and recover from domestic incidents. DSCA is provided in response to requests from civil authorities and upon approval from appropriate authorities. DSCA is conducted only in the US homeland [47] .*

3.4 SmartBase/SmartCity

Smart City Projects are those that integrate IT with the management and operation of civic functions, and OT and public service requirements. The systems upon which Smart City Projects are built can impact virtually every aspect of modern life, including communications, utilities such as water and power, transportation, and government services due to the wide-ranging scope and the amount invested.

A smart city is defined as a framework that incorporates next-generation IT to essentially all areas of CI. An example would be installing sensors into power grids, hospitals, water systems, and so on. In their paper, *Smart City and the Applications,* authors Su et al. explain a smart city as a physical manifestation of the "Internet of Things" [50]. In other words, a city in which everything is connected via cloud computing; a city that can communicate with itself. The goals of a smart city are to sustainably enhance the development of human society and to effectively combat the challenges of urbanization. AI is vital in the pursuit of these goals. For example, incorporating AI into transportation systems can effectively reduce urbanization challenges such as overcrowding, traffic congestion, and environmental degradation [51]. Voda et al. explain this is because AI can effectively relay real-time traffic updates and make sound predictions on when and where traffic will be the most congested [51]." A smart city is one well-equipped with AI in many, if not all, facets.

Enhancing human society is undoubtably important; so too is the necessity of enhancing CIP as technology connects each sector more than they already are. This will require an increase in cooperation between the public and private sectors; the private sector would have to relinquish some degree of secrecy so the public sector may support it, and vice versa. If smart cities are an example of what CI will evolve into on a national or global scale, innovative solutions for CIP are necessary to ensure these institutions cannot be exploited, violated, or attacked.

As technology brings a connectedness to CI in support of smart city initiatives, a high degree of focus will be on the trustworthiness and security of these tools. The inherent risk involved in tying life support functions together is the potential for catastrophic disruption. While there are many functions that can afford to substitute resilience for security, the additional risk to DOD related functions should be assessed differently than civilian infrastructure. It will be vital that the federal government ensures the security of the systems and devices brought into the CI ecosystem that exists to support continued DOD operations.

Instead of always trying to be as close to perfect as possible with regard to all characteristics, designers need to identify a "sufficient level" that supports each characteristic. Determining what qualifies as "sufficient" will depend on the nature of the project. A risk-based assessment can be useful in making this determination, as in any system the failure of some characteristics will be more consequential than others. A system on which public safety depends will need to be very resilient; a system that provides a minor convenience will only need to be resilient enough that it does not annoy people by being offline too often. The question is not whether to support a trust characteristic, but what degree of support makes sense.

Smart city projects are challenging endeavors and can fail or underperform for many reasons, so it is necessary to consider the ways in which each stakeholder will design and in what ways the perspectives are siloed, in order to identify an integrated solution that address the broad scope of smart city projects [52].

The recommendations outlined in this report facilitate an early, important step in the process of developing a smart city system. It is hoped that readers will use the information about key trust characteristics to consider the several ways in which users need to have confidence in a smart city

system and ways in which their smart city project can meet them. By incorporating appropriate levels of support for all trust characteristics, projects mitigate many factors that can lead to failure [52].

The goal of the SmartBase/Smart City initiative is to bring military installations in line with DOD modernization efforts. The initiative seeks to add to force capabilities by enhancing supply chain and logistics, energy use, water use, communications, and other sectors where connectivity will enhance Homeland Defense by keeping pace with surrounding built environments. The hope is that this will also enhance recruiting and retention efforts for all branches [52].

While these initiatives add benefits, they introduce vulnerability through connected IoT devices and ICS. The challenge is also amplified with legacy systems that are integrated into the connected ecosystem.

Connectedness may compromise, but there are stand-alone and decentralized solutions that avoid costly, and increasingly redundant infrastructure which are also inherently more resilient. For example, the use of microgrids to provide energy to disconnected environments is currently being tested at multiple DOD installations, and these utility solutions provide the ability to disconnect from traditional utility power as needed. These microgrids can provide a degree of stability in the face of disasters. There are also solutions to ensure that the cyber components of these microgrids remain secure in the face of intentional disruption/attack.

3.5 State of the Art

The advancement of AI/ML provides the means to rapidly advance science itself. Trained systems can comb through and aggregate entire libraries of scientific documents, looking for particular information, and anomalies. AI image recognition can detect cancer and illness, and potentially even pathogens. Studies can be simulated with increasing accuracy, and financial processes

While not necessarily a technologically advanced solution, decentralization of systems should be noted as state of the art. As a strategy that had not been widely adopted in the past, due to governing philosophy, technology has allowed for a higher degree of command and control, while still allowing for isolation of systemsas needed. The Energy, Communications, Water and Wastewater, and IT Sectors provide examples of how processes and decision-making can be pushed to the edge without being outright disruptive. Cloud computing at the edge, power generation that works to augment Utility and when necessary run in Island mode, and wireless mesh communication in isolated environments demonstrate how similar systems might borrow from the underlying concepts of decentralization.

4

Impact of Disasters on Critical Infrastructure

4.1 Introduction to Disasters, Hazards, and Risks

Disasters are deadly, destructive and disruptive events, which occur when hazards interact with human vulnerabilities. The impact of disasters, whether from natural events, manmade hazards, atypical emergencies, or public health crises, can be devastating. The costs to return to normal are continually rising. Mitigating the impacts of such events "requires a comprehensive plan for effectively and efficiently addressing vulnerability. Yet when doing so, the variety of criteria for success that extends beyond simple dollar-based cost-effectiveness must be considered. Indeed, the broader and more complex societal impacts that include fairness, equity, and responsiveness must be addressed [53]."

It is axiomatic that the more advanced society becomes, the more complex safety issues become. Today's world is filled with more complicated and immediate dangers than ever. Given the tectonic shifts of globalization and the expansion of democratization, the nexus between security and socio-cultural respect presents a variety of policy and administrative challenges [54] [55]. Population growth, alongside economic development, and urban expansion will inherently increase the number of places and systems prone to disasters. The United States faces numerous disasters each year that cause thousands of deaths, costs billions of dollars in disaster aid, disrupt commerce, and destroy homes and critical infrastructure.

Hazards are sources of danger that can lead to an emergency situation and pose a threat to life, health, property, or the environment. Typically, they are categorized into two typologies, 1) natural hazards, and 2) manmade, or human-induced, hazards. Natural hazards are hazards that exist within the natural environment and are considered acts of God, and consist of atmospheric, geologic, hydrologic, seismic, and biologic agents [56]. They are thought to be unpreventable and are associated with a perceived lack of control. Manmade hazards result from human intent, negligence, error, or involving a failure of a man-made system, and consist of sociological and technological hazards. They are not considered predictable although thought to be preventable; hence, their association with a perceived loss of control [57] [58].

Risk is the susceptibility to death, injury, damage destruction, disruption, stoppage, etc. While it may be possible to alleviate some risk to natural and manmade disasters, continued increase in the global population alongside infrastructural development will likely result in an increased risk to hazards [58].

4.2 Responding to Disasters

It is the essential role of government to respond to events, in particular events of significance. This includes:

- Assisting with disaster declarations;
- Providing public and individual assistance as well as matching mitigation funds;
- Activating the federal response plan; and
- Assisting with emergency support functions (transportation, communications, public works and engineering, search and rescue, mass care, etc.).

Therefore, "[c]ritical infrastructure plays a significant role during natural [and other] disasters… preparedness and mitigation strategies should include identifying and fortifying vulnerable infrastructure based on their inter-relationship with the associated industries and communities routes and bridges for evacuation and public buildings for sheltering [59]."

Figure 4-1 displays a disaster impact model, indicating how the three impact conditions of hazard exposure, physical vulnerability, and social vulnerability determine the effects from a disaster, and ultimately the physical and social impacts that will remain following response and recovery activities.

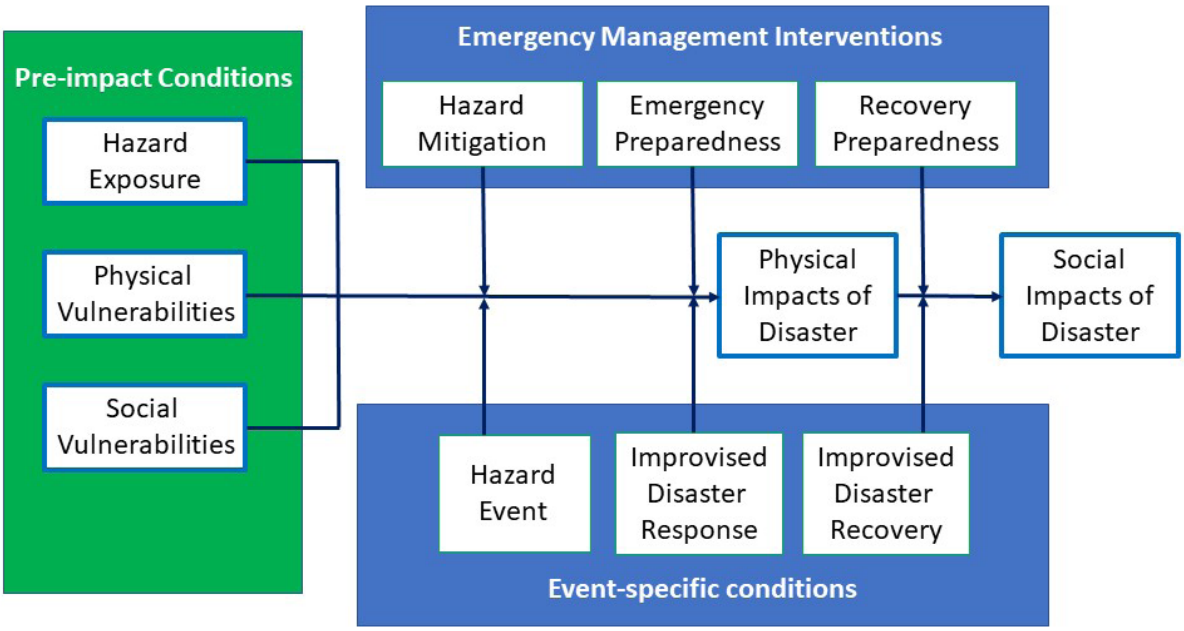

Figure 4-1. Disaster Impact Model adapted from [60].

4.3 The Need for Emergency Management in Homeland Defense

> *The goals of effective emergency management and homeland defense are to reduce, or avoid, the potential losses from hazards, assure prompt and appropriate assistance to victims of disaster, and achieve rapid and efficient recovery. The results will be largely determined by the ongoing process through which governments, businesses, nonprofits, and civil society plan for and reduce the impact of disasters, react during and immediately following a disaster, and take steps to recover after a disaster has occurred. Appropriate actions at all points in the cycle lead to greater preparedness, better warnings, reduced risk and vulnerability, and the possible prevention of future disasters. Effective emergency management and homeland security involves the development of public policies and plans that either modify the causes of disasters or mitigate their effects on people, property, and infrastructure [61]*

To accomplish such measures, emergency management and homeland security organizations must implement plans that:

- Identify, assess, and prioritize local and regional vulnerabilities to emergencies or disasters as well as the resources available to mitigate, respond to, or recover from them;
- Promote collaborative initiatives between public, private, and nonprofit organizations at the federal, state, regional, and local levels to ensure necessary actions are taken to prevent and/or mitigate the effects of disasters, and that they are prepared to respond to and recover from such an incident when an emergency or disaster does occur;
- Provide for the utilization of all available public, private, and nonprofit resources to protect against and respond to an emergency or threatening situation;
- Provide for the utilization and coordination of local, regional, state, and federal programs to assist victims of disasters and prioritize addressing the needs of the elderly, disabled, poor, and other groups that may be especially affected; and
- Provide for the utilization and coordination of state and federal programs for recovery from emergency or disaster situations with particular attention to the development of mitigation action programs [53]

4.4 Review of Disasters

The wide variety of disasters can pose an ever-challenging risk to various CI. This section will provide a brief review of disasters that have occurred and discuss some of their impacts.

4.4.1 Extreme Weather (Hurricanes, Deluges, Tornadoes)

Extreme weather events have the ability to impact every sector in CI, and the impact of weather events on CI is an ongoing challenge. Hurricanes and tornadoes, flooding, earthquakes, and wildfire can damage structures, interfere with routes used for logistics and access, and cut communications used for sharing information, as well as conducting command and control at incident sites.

Hurricane Sandy, the Category 3 storm that impacted the mid-Atlantic coast in the fall of 2012, wreaked havoc on infrastructure that was not designed to take the force of the storm's impact. From public housing to wastewater treatment, the severity of the storm was felt by the populations of the

impacted and adjacent areas in nearly all aspects of their lives. Similarly, Hurricane Katrina, in 2005, devastated the Gulf Coast, crippling New Orleans. Hurricane Michael, in 2018, impacted Houston. The concern of increasingly erratic and massive storms in the future has spurred debate about what resilience looks like, especially for those adjacent to coastal areas.

Unfortunately, the majority of planning is designed as reactive to an event, instead of proactive and preparatory. The policies and procedures around requesting federal aid do not allow for federal proactive responses and given the private ownership of the majority of CI, it is not the federal government's responsibility to ensure resilience.

4.4.2 Manmade (Oil Spills, Nuclear Meltdowns, Dam Failures)

Critical Infrastructure supports the daily life of the citizens of the United States. It requires continuous monitoring and maintenance to ensure smooth operations when the various sectors are most needed. Unfortunately, not everything goes without a hitch. While there are always efforts to mitigate these circumstances, planning for human error is never foolproof. Checklists, processes, and procedures are implemented to allow for the complexity of operations; however, they are prone to human-error with the result being manmade disasters. A brief review of nuclear accidents, oils spills, and dam failures reinforces the role that humans have in preventing disasters.

Many people think that Three Mile Island, in 1979, was the first nuclear disaster in the United States. While it received a lot of attention, due to its proximity to large population centers including New York City, there was an event that predated this event by almost 20 years. In January 1961, near Idaho Falls, Idaho, a 3 megawatt experimental power reactor experienced a prompt critical excursion (an instant surge to full power) when the central control rod was improperly removed. The three operators who were present were killed. This event demonstrated the importance of designing safety into the reactors, given that this is the only nuclear reactor event to have resulted in immediate fatalities in the United States.

During the 1990-1991 Gulf War, the retreating Iraqi Army opened the oil valves to the Kuwaiti Oil Reserves, dumping approximately 8 million barrels of oil into the Persian Gulf. This intentional act of sabotage against Kuwait resulted in an oil slick approximately 350 square miles in size. While the economic impact of the event was immediately disruptive, the environmental impacts are still being observed more than 20 years later [64].

More recently, the Deepwater Horizon oil spill in 2010 occurred when the cement casing at the base of the Deepwater Oil Rig in the Gulf of Mexico cracked, allowing crude oil and natural gas to escape, reaching the platform, resulting in an explosion that killed 11 crew members on the rig. The cascading failures were the result of inattention to the details, including cement formula and pressure readings [65].

The Dam Sector includes not only the dam structures themselves, but also the hydroelectric power generation stations, levees, and hurricane barriers. The worst dam collapse in U.S. history is the Jonestown, Pennsylvania flood of 1889. The uncharacteristically heavy spring rains and inadequate maintenance coalesced into a disaster that resulted in the deaths of 2,200 people, and the destruction of an entire town in western Pennsylvania.

4.4.3 Terrorism and High Threats

The U.S. Code of Federal Regulations defines terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives [66]." The deadliest terrorist attacks on U.S. soil occurred in September 2001 when hijackers flew airplanes into the World Trade Center twin towers in New York City, the Pentagon in Arlington, Virginia, and a field in Shanksville, Pennsylvania. The resulting loss of life numbered in the thousands, the cost to rebuild infrastructure and various building was in the billions of dollars, and the total economic impact is likely an incalculable number.

According to the 9/11 Commission, "the most important failure [in the September 2001 terrorist attacks] was one of imagination" on the part of the intelligence community [67]. Policymakers have attempted to reduce the impacts associated with terrorists and other attacks by anticipating the unexpected; however, it is easy to under-analyze the complexities of public safety [68]. First, threats occur within fairly narrow settings and a limited geographical scope, which prohibits policymakers from making sound solutions. Second, traditional disaster management models developed by policymakers have typically focused on post-crisis response and recovery lessons learned from terrorist attacks, diverting attention away from evaluating current practices or adopting new procedures until there is an imminent crisis [69]. And, third, policymakers are unequipped to handle many of the economic, health, and environmental elements of attacks, as well as incapable of fully seizing many of its social and political attributes [70]. Thus, given the limited opportunities for crisis-related experience, "decision-making, mental models, and situational awareness research on [crises] have highlighted a further need for effective emergency management [71]." Understanding the meaning, causality, severity, and incidence of threats, both implied and actual, is essential to the public safety problem-solving process [72].

4.5 Summary

The implementation of successful strategies for emergency management and homeland defense require a process that is adaptable to the landscape of changing threats and emerging ideas. For example, the threat presented by terrorism is shifting at a rapid pace. Terrorists can change their methods and targets swiftly, often resulting in displacing vulnerability to less protected sites. Or, as another example, the impacts of global climate change, while readily evident, are not fully understood and defensive strategies have become highly, even caustically, politicized.

The trend toward greater infrastructure interdependency in the United States has accelerated in recent years and shows little sign of abating [73]. The importance of identifying, understanding, and analyzing these infrastructure interdependencies must be recognized for effective disaster response.

The truth is that few infrastructure systems currently maintain any substantial level of excess capacity or redundancy in their systems. In 1981, Choate and Walter published *America in ruins: The decaying infrastructure* in which they assert that the United States was seriously underinvesting in its infrastructure and that the infrastructure was wearing out faster than it was being replaced [74]. Despite receiving widespread publicity in the 1980s, not much has changed in the intervening years. The combination of disasters, such as on the scale of a Hurricane Katrina, and complex, interdependent, aging infrastructure points to making investments in infrastructure systems a national priority [75].

5

Predictive Modeling for Critical Infrastructure Protection

5.1 Introduction to Predictive Modeling

Predictive modeling looks to predict outcomes by using statistics. As with any modeling endeavor, the predictions are a function of the input data, with better data resulting in better predictions. Data is a strategic resource in today's competitive world. Data mining and warehousing is the nontrivial extraction, analysis, and management of implicit, previously unknown, and potentially useful information from complex datasets or databases. Although data mining and warehousing is an umbrella term for the compilation and integration of datasets to generate new information about a wide range of contexts, it is typically associated with the need to identify trends and predict future thoughts and behaviors permitting for proactive decision-making, similar to AI [76] [77]. Prior to data mining and warehousing, it was nearly impossible or exceedingly difficult to keep track of huge amounts of details. Several powerful tools and technologies support data mining and predictive modeling include Geographic Information Systems (GIS), Geointelligence, and Computational Statistics.

5.1.1 Geographic Information Systems

A GIS is a program used to create and manage geospatial data and its associated attributes, by integrating, storing, editing, analyzing, and displaying geographically-referenced spatial and temporal information. GIS data represents real-world objects (roads, land use, elevation) with digital data. Real world objects can be divided into two abstractions: discrete objects and continuous fields [78]. The

use of GIS is ever-expanding—the capacity for it to manage and process data this way distinguishes it from other programs, making it a valuable tool for CIP with a wide variety of applications [78]. As developments of the system continue to improve, they will, in turn, result in much wider use of the technology throughout science, government, business, and industry, with applications for every CI sector. GIS has also proven to be beneficial when used in coordination with other technologies, thus becoming a synergetic technology, especially in the areas of public safety, national security, and homeland defense [76] [79] [80].

5.1.2 Geointelligence

In order to meet the difficult challenges of risk assessment, mitigation, preparedness, response, and recovery, data analysts have begun utilizing a concept that uses not only data mining and warehousing but satellite imagery and GIS. Geointelligence is "this transition toward the digital era [that] is characterized by the [collection and] spread of information and knowledge technologies, globalization, and networking activities [81]." More specifically, this technological innovation provides geospatial processing and an open environment for integrated geospatial production, which aims at aggregating and analyzing informatics "to improve national security [82]." Thus, by using a variety of information, geo-intelligence specialists are capable of running powerful GIS through several layers of digital geospatial data to render map-like products. "Informatics responds to the reality that human analysis is not 'scalable' – there is just too much raw data for an analyst, or an army of analysts, to process manually. One solution to [data management] is to surround human analysts with 'machine reasoning' tools that augment human capacity [83]."

5.1.3 Computational Statistics

Computational statistics, or statistical computing, is a newly developed goal-oriented paradigm that uses computer technology, operational strategy, and managerial accountability to structure how organizations provide services [84] [85]. The process combines several philosophical themes including reform and problem solving, hierarchy and leadership, and control and creativity. "Leaders reform their approach to managing their resources and at the same time promote local problem-solving. Hierarchy is reestablished and reaffirmed…, whereas command, supervisory, and line officers are simultaneously exhorted to do whatever is necessary to respond to identified problems… and, to the issue of control and creativity, it juxtaposes these elements by "making sure things are under control" while also maintaining support for local initiatives [86]." Computational statistics also serves as a *great theater* for organizations in effectively communicating ideas and strengthening relationships with the public, the media, and internal members [87].

5.2 Embracing the 4C's – Communication, Coordination, Cooperation, and Collaboration

In every endeavor to protect and secure CI it is necessary to begin by assessing the environment. The challenge presented in CIP begins with forming strong relationships with other government agencies and with private industry and other public and nonprofit partners. Understanding the meaning, causality, severity, and incidence of threats, both implied and actual, is essential to the problem-

solving process. Given the limited opportunities for crisis-related experience, decision-making models have highlighted a need for collaborative partnerships. Information sharing is, therefore, a critical need for the effective and efficient administration of response activities. Increased communication and enhanced coordination and cooperation in times of threats should, therefore, be recognized as important and viewed as a relevant means to ideological bridge-building that aims to strengthen social cohesion and political confidence [88] (See Figure 5-1).

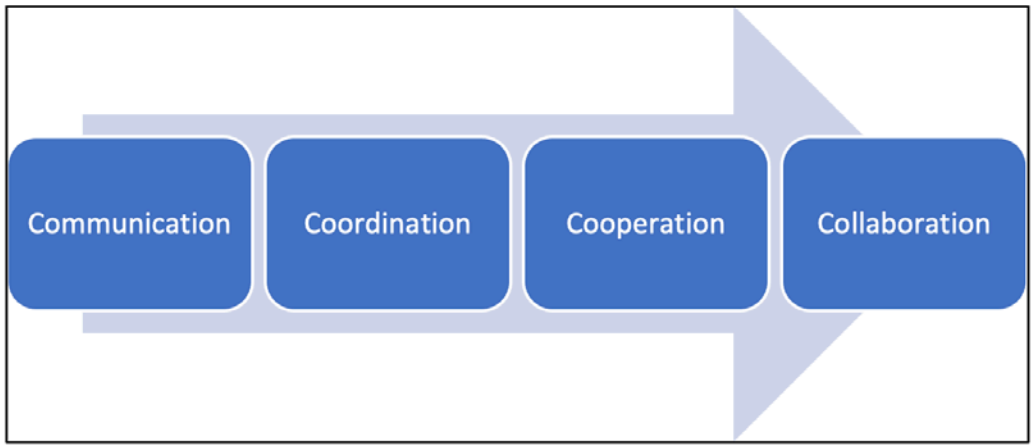

Figure 5-1. Thornton's 4C's Model [89].

5.3 Simulating Interdependencies

Another area to consider, when simulating interdependencies is the Herfindahl-Hirschman Index (HHI) for market concentration. While traditionally used by financial analysts to gauge market concentration and competitiveness, this tool can also be useful for providing insight into risks around economic sectors. While not focused on the Financial CI Sector, it offers a model of vulnerability to areas of CI and their potential interdependencies.

For example, a significant concentration of rare-earth (RE) metal mining and production is found in China. Holding 84% of the market share of REs, the threat to global production of the majority of new technology cannot be overstated. The problem runs much deeper than simple market share when considered in the light of CIP, as the cascading effects of a restricted supply of REs would disrupt the Critical Manufacturing, Communications, DIB, and other CI sectors. It would also provide an advantage in distancing capabilities, compounding the effect of the disruption well into the future. The model can also be used to inform decision making around vulnerabilities in workforce availability.

In another case, looking at the COVID-19 pandemic, the Food and Agriculture Sector provides another example. The consolidation of food production into large processing facilities to drive production and profitability has resulted in a concentration of workforce populations. The unintended consequence of this consolidation during the pandemic was the near shutdown of the U.S. Department of Agriculture (USDA) approved meatpacking facilities, due to a concentration of cases within the workforce population. The issue is compounded because Food and Agriculture, a CI sector, requires workers, designated as essential employees, to work despite the increased danger of exposure to the COVID-19 virus.

These vulnerabilities draw attention to the need to consider the role that decentralization of geographic locations and the role of foreign corporations have within CI. By including the HHI and other models in the assessment and evaluation of CI sectors and supply chains, informed decisions can be made with regard to policy and regulation.

HHI models of market concentration can be integrated alongside other data-sets, such as business ownership information, supply chain and logistics, raw material inputs, and even maintenance records. The resulting tools can be developed that assist in proactive planning for natural disasters and intentional and accidental manmade events [89] [90].

5.4 Summary

A new revolution of information technology is underway. Now, more than ever, the federal government and private sector are creating, collecting, and storing data. Better intergovernmental data will help the various levels of government better understand the scope and scale of the issues to be addressed and the resources available to evaluate CI vulnerabilities and improve CIP.

VOLUME II

6

Cybersecurity Principles and Technology for a Power Utility Substation Automation System

6.1 Introduction to Substation Automation System

A Substation Automation System (SAS) is a substation monitoring and control solution that provides protection, control, automation, monitoring, and communication capabilities. Cyber-Physical System (CPS) represents a paradigm shift in engineering secure solutions. This paradigm shift comes as Internet protocol connected systems and components become increasingly prevalent. An engineering design solution using cybersecurity principles and techniques must meet the objective of operational-relevant, near-real-time defense of sensitive information and processes accessed using IT associated with an OT electrical substation. IT deals with information while OT primarily deals with machines, or the physical realm (i.e., physics-based system health rather than data network traffic such as power, flows, and voltages). The physical realm is associated with what is happening on the power side. Cybersecurity presents the alerts to a cyber system such as network information about cyber health data that could be physical indicators. Newer technologies such as Software Defined Networking (SDN) solutions are matured to impressive Technology Readiness Levels (TRL). Such technologies deliver possibilities of new capabilities transitioning from entirely manual processes, to human-in-the-loop, and eventual fully automated Courses of Action (COA) without human intervention. As will be discussed throughout Volume II, the More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD) will transition a fielded prototype of such a capability, including automated workflows, a control system baselining tool, a reference architecture (RA), training plans, guidance on system interfaces, as well

as other systems engineering artifacts for reuse. A power utility SAS interface to the Internet creates a radical shift, with the need to rethink how cybersecurity principles and techniques are applied to physical system interfaces and power utility system environments.

System engineers are tasked with designing, developing, implementing, and managing complex, large-scale systems throughout the entire life cycle. The convergence of Information IT and OT, or the Industrial Internet of Things (IIoT), also referred to as Industry 4.0, is happening at an accelerated, broader scale than ever before. Industry 4.0 creates a cyber capacity affecting all system-level elements used in the operational side of Facility Related Control Systems (FRCS). High IT and OT convergence affect system connectivity, data, and information elements that introduce cyber resiliency challenges to the operational technologies system. An information-enabled electrical SAS for power utility today may have many interfaces with the Internet. However, the OT operational context is different from that of an IT system. In addition to operating within a different environment, OT operators respond to operational anomalies differently than IT users. Adversaries target CI assets (such as power, fuel, water, and critical facilities) using cyber-attack vectors. Therefore, systems must be engineered using cybersecurity principles and techniques formulated and tailored to such an environment's unique characteristics, keeping in perspective all systems-level elements (including people, hardware, software, facilities, policies, documents) that produce desirable system cybersecurity results.

A power utility SAS is an example of a system to which to apply cybersecurity principles and techniques. SAS emerged in the mid-1980s, and SAS advancement commenced in earnest with the establishment of communications within substations in the early 2000s. The major break-through in SAS occurred with the introduction of interoperability of applications and the introduction of standards such as International Electrotechnical Commission (IEC) 61850 (IEC 61850) for the design and implementation of SAS [91]. IEC 6180 is a standard for the design of electrical substation automation, and IEC 61850 provides an RA for electrical power systems, enabling interoperability among vendors to support system lifecycle maintenance and sustainment. Part of IEC 61850 is the Substation Configuration Language (SCL) used to exchange information independently of a manufacturer [92]. Adversaries can target CI and FRCS (such as power, fuel, water, and other critical facilities) pertaining to Industrial Control Systems (ICS) by cyber-attack, and SAS requires defensive hardening against such cyber-attacks. Using cybersecurity principles and techniques as part of the systems engineering of a SAS formulated and tailored to the unique characteristics of a power utility information-enabled enterprise electrical environment presents a way to achieve system resilience. This approach also helps to defend sensitive information and critical infrastructure processes against attacks by malicious parties or unintentional cyber events. Cybersecurity enables cyber defenders and facilities engineers to identify, respond to, and recover from asymmetric attacks in mission-relevant time on CI.

6.2 Overall System Nature, Purpose, and Functions

The overall system nature, purpose, and functions of a power utility SAS is to support an electrical system's operations. Its purpose is to generate, transmit, and distribute electricity with utility and warranty for the customer. A SAS is a substation monitoring and control solution that provides protection, control, automation, monitoring, and communication capabilities. The conceptual design of the electrical SAS is based upon a power plant facility that generates electricity. Electricity is sent to the transformer where it is stepped-up, goes through transmission lines to the receiving transformer, and stepped down for voltage use. The substations in the transmission grid interconnect with external interfaces as part of the electrical infrastructure. There are several types of substation that may be

classified by the voltage (i.e., high voltage, extra high voltage, or ultra-high voltages) or service rendered (i.e., transformer for transforming voltage, switchyard for switching between substations, or customer for power distribution to customers). For example, the system substation transfers bulk power across the generators' network to load centers, providing switching facilities, power transformation, and voltage conversation. The switchyard substation connects the generators to the utility grid and provides off-site power to the plant. The distribution substation supplies power to consumers. The customer substation is the primary source of energy to the consumers. The system, switchyard, and distribution substations are typically more extensive, more expensive to construct, operate and maintain than customer substations built to purpose dependent on the customer's electrical power needs (e.g., businesses or residential homes).

The functions of an electrical SAS support sensitive information and processes of these power utility substations. The SAS performs these functions with the use of computing and communication technologies. Types of substations used in the transmission and distribution of electrical power include system, switchyard, distribution, and customer substations. New technologies and data communication techniques have advanced the use of automation in traditional power systems that previously primarily operated using manual controls. The nature of an electrical SAS needs to be designed to ensure confidentiality, integrity, and availability of power utility information. Substations are used in the transmission and distribution of electrical power. Component devices integrated into the electrical grid require physical and cyber protection to ensure uninterrupted operation. The electrical SAS provides the capability to identify security threats, respond to security events without human intervention, deploy, and make changes to system model and hierarchical management architecture. This capability can be also be applied to defend other cyber-physical system sectors such as water, fuel, or facilities. The SAS functions can be used for monitoring cybersecurity functions such as information gathering on alarm contacts indicating unauthorized network access, time-stamped record of change-of-state events, metering and monitoring functions, network traffic monitoring, or alerts of abnormal power system conditions during suspected cyber events. Other SAS functions provide data that may be used as information in the following ways: advanced data analytics with consolidated visualization views of operations to minimize risk and optimize electrical power distribution, marketing analytics, asset performance analytics, energy management and forecast performance, metrics such as load and price forecasting to predict electricity consumption and prices, power grid analytics to reduce the number of unplanned outages and optimize maintenance, and regulatory compliance reporting requirements end-user analytics such as customer demand.

Primary system users of an electrical SAS perform operations in support of power distribution operations. Users work with teams of specialized engineers and designers involved in design and project management of distribution and electrical power transmission. SAS users monitor operations and support project management activities. System users include personnel in the power supply organization. For example, executives responsible for directing operations related to electrical power supply and electricity marketing functions may use the SAS for information to develop reports. Plant managers accountable for operations management and directing procurement and contracts associated with the substation are SAS users. Personnel such as contract administrators responsible for managing contracts may need to access sensitive information from the SAS. Quality managers who are accountable for quality assurance testing. Energy coordinators responsible for dispatches and wholesale merchant power functions may also use it. The access list of primary system users may include substation managers responsible for directing personnel that design, construct, and maintain transmission substations. Other system users may consist of personnel performing various system functions, such as the grid manager, electrical power systems engineers, substation engineers, field

services engineer, power systems control engineer and protection/test technicians, power delivery operations support, a power distribution engineer, or systems engineer.

6.3 External Interfaces

Secure and dependable operations of an electrical SAS include many cyber and physical interfaces, making the security of systems vulnerable to cyber threats and incidents. Power utility systems are engineered for dependability, and only recently is cybersecurity engineering being built into the system architecture. However, the cyber threats are relatively the same as for IT. The topology of a power utility SAS includes automatic substation breakers and human control loops, field device sensors, and protected endpoints using separate Virtual Local Area Networks (VLANs) for remote diagnostics. The necessary equipment and external interfaces for an electrical SAS include: distribution transformer, circuit breaker, Air Break (AB) switches; primary power lines; ground wire; overhead lines; circuit breakers; current transformers; Level 1 field devices (e.g., relays, meters, Remote Terminal Units (RTU), Programmable Logic Controllers (PLCs)); Level 2 Substation data concentrator; Level 3 SCADA system/data warehouse; substation processor; Safety Instrumented System (SIS)/protection relay; substation Local Area Network (LAN); Human-Machine Interfaces (HMI) (e.g., user interfaces); communication interfaces; control server, data historian; and engineering workstation.

6.4 Substation Automation System Cybersecurity Environment

The SAS cybersecurity environment also has HMI at user workstations and interfaces to enclave servers, storage, and peripherals. In contrast, other devices such as system and network servers, support typical applications such as Email, system data, user accounts, access control lists, traffic monitors, system administration, and security tools. Additionally, network components such as routers, modems, and remote access points are to be used in the architecture to control and monitor remote control center interface functions. As CPS become more interconnected with business networks, the threat vector of connection to the Internet increases the potential vulnerability for remote cyber-attacks. Network connection to the Internet is not the only prerequisite to an attack on OT. CPS is vulnerable to exploitation at the PLC level, which controls the physical processes.

PLCs and other end devices were traditionally designed to be used in closed network system environments. PLCs can be programmed using ladder logic, or customized programming to provide an interface for users to control physical interface inputs between devices and machines, or human-facilitated inputs (e.g., button-pushing, switching, keyboard inputting). The outputs start functions such as turning a mechanical process on or off. Traditional substation designs use Ethernet, a physical networking protocol, while more modern design uses Ethernet/Industrial Protocol (IP) switches for communications. The Ethernet/IP is a standard industry communication protocol used at the application layer of the architecture. A ring topology is used to ensure redundant paths and reliability. This approach is quite different from emerging SDN solutions. The use of legacy Ethernet or Ethernet/IP may soon be dramatically changed by introducing SDN capabilities. The traditional Ethernet control plane is located in the network appliance hardware (e.g., switches). In contrast, SDN is found in software called a flow controller [93]. Switches transmitting different per-flow requirements vary signal transmission performance. Transmitting delay-sensitive user flows with shorter end-to-end

delay and control plane delay are highly desired attributes. SDN advantages include improved network traffic control capability, reduced network resource consumption, and balanced link loads. Today's limitations are the economic, technical, and organizational challenges of integrating SDN into the utility SAS architecture and design [93].

6.5 Graphic of a Power Utility Substation Automatic System

Given the near-term, anticipated changes to a power utility SAS due to the cyber environment begs the question, "what does a typical electrical SAS look like today?" A graphic of a power utility information-enabled enterprise SAS is shown in Figure 6-1 . Ideally, boundary areas of sensitive information are protected by enclaves, Local Area Networks (LAN) and Unified Threat Management (UTM) appliances, and firewalls from external Internet, Wide Area Network (WAN), and Cloud communication. Untrusted devices such as wireless routers communicate through protected endpoints using separate VLAN domains. Less secure support networks reside outside the protected enclaves, separated by firewalls, LAN, and UTM to control traffic flows. System and network servers communicating with substations are also designed to protect sensitive information and processes located in the enclaves using firewalls and LAN switches and routers. The entirety of the power utility information-enabled enterprise SAS requires a holistic cybersecurity defense approach to achieve system resilience and better defend sensitive information and processes against malicious attacks or unintentional cyber events.

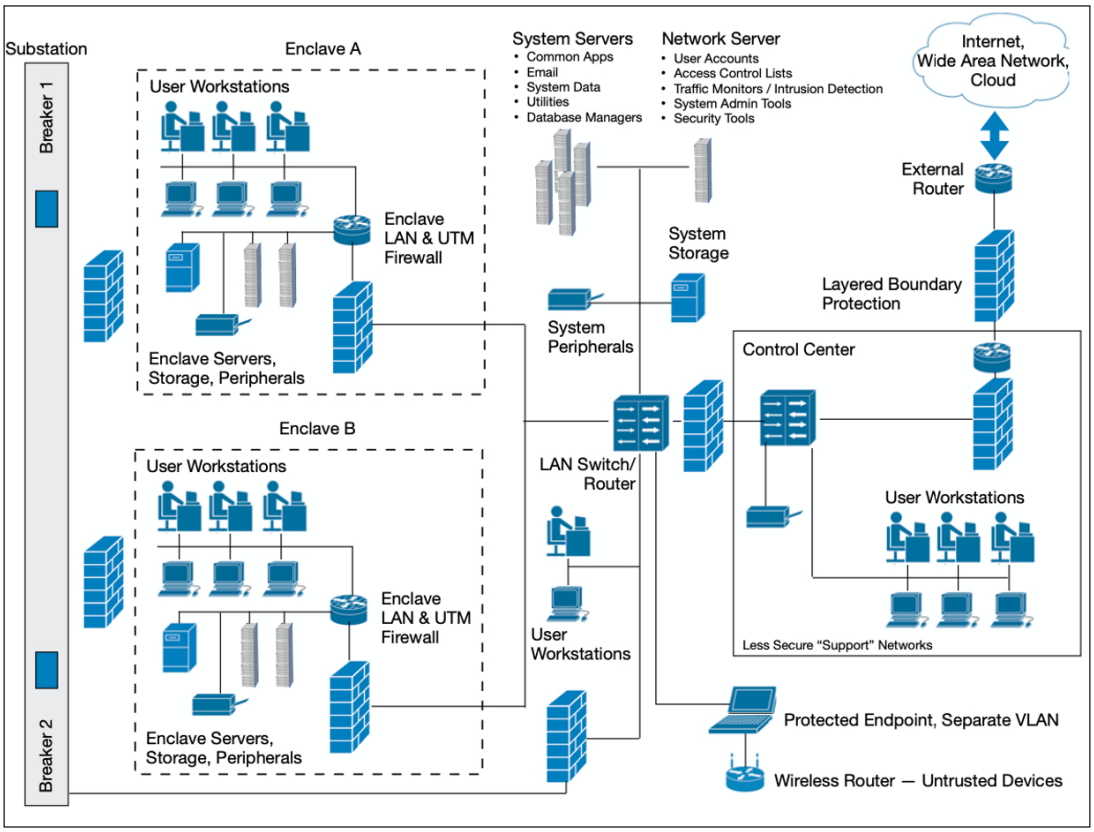

Figure 6-1. Anatomy of a Power Utility Information-Enabled Enterprise Electrical Substation Automated System (Source: Authors).

Network security of a SAS is about restricting access to the system's logical areas using enclave

security zone, applying firewall rules, using access control lists, and then using Intrusion Detection Systems (IDS) to segment or micro-segment sensitive information and process zones that require monitoring and protection from less secure zones. Continued monitoring for network detection and response is a required capability of SAS. Similar to an IT enterprise system, continuous SAS monitoring of data entry and exit points between trust boundaries can be achieved using a combination of a Configuration Management (CM) system and a logging center. The distinction is in the automation.

In 2019, an entirely new industry referred to by industry researcher Gartner as "SOAR" emerged around the requirement of continuous monitoring of data entry and exit points. Trust boundaries introduced greater automation of processes and response to alert detection [94]. Security, Orchestration, Automation, and Response (SOAR) technologies enable organizations to collect and monitor inputs in a digital workflow format. SOAR is quickly being adopted in IT enterprise network environments and is being leveraged in the power utility sector's research efforts. This SOAR technology is a stepping stone towards the use of SDN capabilities. SOAR offers accelerated incident response times, increased accuracy across security operations, and significant time and cost savings to respond to alerts. Some commercial vendors claim that the average response time to system alerts can be reduced from 30 minutes or more to less than five minutes, which equates to approximately 83 percent of time saved per alert (See Figure 6-2).

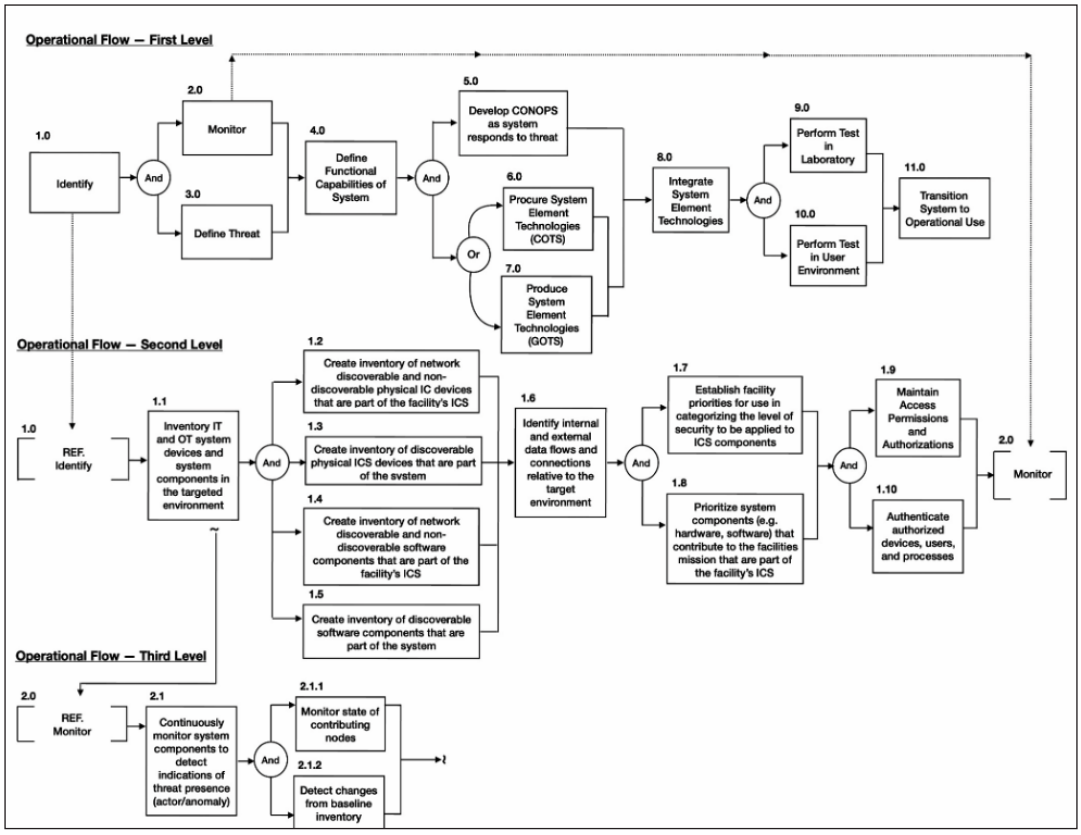

Figure 6-2. Power Utility Substation Automated System Data Flow (Source: Authors).

6.6 Summary

SAS interface to the Internet creates a radical shift, and the need to rethink how cybersecurity principles and techniques are applied to physical system interfaces in power utility system environments. United States Indo-Pacific Command (USINDOPACOM), North American Aerospace Defense Command (NORAD), and USNORTHCOM articulated the urgent need for defensive capabilities of ICS for mission assurance of critical infrastructure. The MOSAICS JCTD is the first response to a demonstration of the first operational capability to enhance security. When MOSAICS capability is demonstrated in 2021, MOSAICS will provide cyber vulnerability baselining, enhanced asymmetric threat indications and warnings, anomaly detection, and information sharing capabilities within an automation framework that enables real-time response actions to disrupt attacker kill chains, timely recovery to restore normal operations, and machine-to-machine sharing of threat indicators and mitigations to degrade adversary reuse of attacks for a power utility system. The operational value to the warfighter is an enhanced understanding of risk to critical infrastructure and supported operational capabilities, the ability to detect control system threats faster from months to minutes, improved situational awareness driving real-time decision aids to enable cyber defender response, disruption of the adversary kill-chain in mission-relevant time, ability to limit adversary reuse of attacks through enhanced sharing of indicators and mitigation, and an application of referenced open-system architecture across the Services [95].

As IIOT disrupts the CPS domain, the initial observation is that there are not enough cyber trained personnel to manage these connected systems. Further research is needed to identify the Knowledge, Skills, and Attributes (KSAs) and experience required by an IT/CPS workforce to ensure organizations are well prepared to design, operate, maintain, and sustain future utility SAS. The lack of trained personnel against growing cybersecurity attacks is one reason it becomes necessary to move towards automation and why cybersecurity presents the systems engineering design and architecture challenges for CPS such as an electrical SAS for the power utility. Using cybersecurity principles and techniques as part of the systems engineering of a power utility SAS formulated and tailored to a substation environment's unique characteristics provides protection, control, automation, monitoring, and communication capabilities. This approach presents a way to achieve system resilience and better defend sensitive information and critical infrastructure processes against attacks by malicious parties or unintentional cyber events.

7

Industrial Control System Cyber Defense

NORAD and USNORTHCOM are complementary yet distinct commands that operate under the auspices that our homeland is no longer a sanctuary. Threats include a resurgent Russia, an assertive China, North Korea, Iran, natural disasters, Arctic development, Chemical Biological, Radiological and Nuclear (CBRN) threats, transnational networks, space, and cybersecurity.

The DOD is countering these threats while simultaneously balancing fiscal constraints and difficult economic choices in a rapidly evolving battle space. Joint All-Domain Command and Control (JADC2) and the MOSAICS JCTD are two of the initiatives NORAD and USNORTHCOM are supporting as part of the Strategic Home and Integrated Ecosystem for Layered Defense (SHIELD).

7.1 Critical Infrastructure Interdependency

The USNORTHCOM AOR uniquely encompasses 86 percent of all US military installations with 113 continental United States (CONUS) installations supporting the NORAD and USNORTHCOM missions in defense of the homeland. Additionally, given the globally integrated defense enterprise and dynamic sourcing, the USNORTHCOM AOR, which includes the DIB, is the forward projection point for supporting the remaining 14 percent of installations outside the CONUS. The CI supporting the AOR is primarily a public/private interdependence with the bulk of USNORTHCOM AOR installations dependent on private sector CI, which includes fuel delivery, electricity, natural gas, water, sewage, waste removal, and transportation. Losing the support of the private sector infrastructure within the

USNORTHCOM AOR could significantly impact employment of DOD capabilities worldwide, which highlights the NORAD and USNORTHCOM concern for defense of ICS for mission assurance of critical infrastructure.

7.2 Scenario for a Cyber Attack on Critical Infrastructure

A possible scenario for an ICS attack could unfold as follows: A nation state actor makes a limited attack on a regional peer with the intent of achieving a specified goal (occupy a territory, overthrow a section of government, recover military assets, etc.). Due to supporting treaties and alliances, the nation state actor also understands that the United States may counter this aggressive action with a military or economic response. To pre-empt the U.S. military response, the same nation state actor could launch a pre-emptive first strike in the form of an ICS-based attack on targets within the United States that could slow U.S. capability to dynamically source forces to the conflict area. The ICS attack could be against seemingly innocuous targets, resulting in a slowed response or denial of access or capability at key locations that inhibits force generation. Examples could include disabling the controls on a moving draw bridge to slow transportation at a port facility, disabling commercial electrical power production and distribution, or causing a dam failure and subsequent flooding by disabling the dam spillway operation. The targeting opportunity for ICS controls are endless, especially when considering first, second, and third order effects and the interdependence of CI discussed in previous sections.

If this example is taken further and more specifically, an ICS attack on the 90 percent privately owned commercial energy sector (supply and/or distribution) may yield the desired negative impact our adversary wants to achieve. This type of attack may slow the ability to respond just enough to achieve the adversary's objective before U.S. military forces are able to significantly mobilize their military projection platform. While much attention has been given to backup power for primary facilities (first order effect), the secondary supporting facilities and adjacent supporting communities housing the employees who generate capability may be neglected. If a city housing a significant military community were to lose power, how many people would miss work because daycare and/or schools for their children were closed? How many personnel would be late to work because the alarm did not go off in the morning? How quickly would that power outage impact cellular communications (second order effect), the water supply, sanitation, fuel or food delivery and storage? Generally speaking, private sector infrastructure is highly reliable under normal operating conditions; given that private sector decisions regarding redundant supporting systems are economically derived, redundant systems are minimal, have limited capacity, limited depth of operation, limited duration, and are considered temporary stop-gap measures until a permanent repair is put in place. A long-term electrical outage (several days or weeks) will have multiple second and third order effects impacting DOD mission capability. While system redundancy and contingency planning for key and essential facilities is crucial, it remains vulnerable to second and third order effects that may be difficult to defend against without significant investment in cyber defense. This is especially apparent when a significant percentage of the utility infrastructure supporting military projection capability is computer controlled and resides within the private sector.

As the United States dealt with the COVID-19 pandemic in the homeland, numerous media outlets reported adversaries increasing military activity (flight interceptions at borders) and malicious cyber activity to probe for weaknesses and opportunities in an attempt to gain a strategic advantage during the deadliest pandemic in the last 100 years. Taking advantage of this type of opportunity (or generating this type of opportunity) is to be expected as an adversary is highly unlikely to make a direct kinetic

attack against U.S. CI for a wide variety of reasons. ICS attacks are a limited form of warfare with a low entry cost and a high return on investment that typically results in limited casualties. They can also be difficult to trace back to the perpetrators, which allows for denial and disinformation. Disinformation campaigns may result in doubts, wide swings in public opinion, impacts on the political spectrum, and muddies the waters on perspectives of an appropriate U.S. response to an ICS attack on infrastructure. In the end, the repercussions for the perpetrator are a risk with limited negative consequences while still meeting their desired outcome (slowed U.S. military response).

7.3 More Situational Awareness for Industrial Control Systems

NORAD and USNORTHCOM recognize that threats to ICS have steadily increased over the past 10 years. In an effort to limit the ICS attack surface and counter the threat, USNORTHCOM, along with USINDOPACOM, the Office of the Secretary of Defense (OSD), the DOE, National Laboratories, the military services, and industry partners teamed to develop the MOSAICS JCTD as a step toward mission assurance and ICS resiliency. JCTDs examine new technology for military purposes through operational usefulness, technology capability, scalability across a broader spectrum, and inter-service integration. This allows the services to solve important military problems and transition technology from prototypes to widespread implementation and employment across the military. The operational objective of the MOSAICS JCTD is to resolve cybersecurity risks to ICS supporting DODCI. Overall, the MOSAICS JCTD scope consists of seven key areas to engage ICS threats which includes detection, mitigation, visualization, analysis, decision, recovery, and data sharing of ICS threats with partner agencies. MOSAICS baselines the ICS network, highlights potential vulnerabilities and semi-autonomously identifies, responds to, and recovers from asymmetric attacks on CI, operating at the speed of relevance timeframes. MOSAICS also provides intrusion detection, plus indications and warnings that nefarious actors may be leveraging an ICS disruption as a precursor or in conjunction with other actions to disrupt military capability.

Simply stated, the MOSAICS JCTD technology approach is an integration of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) technologies for enhanced situational awareness and defense of ICS assets within the DOD and the public/private CI. MOSAICS establishes a network baseline, determines vulnerabilities, and monitors for changes in equipment, network, or status. MOSAICS conducts ICS system simulations and integrates current technology with the ability to integrate future advanced sensors for evolving open source system capability. Through automation and autonomy, the system reduces the decision response timeline for system interruptions from months to minutes, disrupting the adversary kill chain in mission relevant timeframes. Through information sharing, MOSAICS minimizes the re-use of adversary tactics, techniques, and procedures (TTPs) and malicious software in executing ICS infrastructure attacks against the homeland. MOSAICS system analytics use AI and machine learning to sense disruptions and determine focus areas for future system development to enhance system integrity and security orchestration. All of this is viewed through customized human-machine interfaces providing visualizations to best communicate intrusions as they occur to the human in the decision loop, resulting in improved situational awareness with real time decision aids to enable cyber defender response and speed to decision.

The MOSAICS team conducted a thorough analysis, detailed feature categorization, and corporate representative product team engagement to document technology capabilities of more than 250 COTS-based ICS technologies. This review was accomplished by several National Laboratories to down-

select technologies using weighting criteria with the goal of meeting all technology gaps with COTS technologies. Initial gaps were identified in end-point sensing, analytics, and visualization. A social media call for developers from the COTS vendor community was made with the intent of seeking gap filling technologies. GOTS technologies were identified to fill some of the remaining technology gaps. The MOSAICS JCTD has evolved into the foundation for the most advanced new technology and TTP integration to further indications and warnings, monitoring, analysis and tracking, and mitigation and defense from ICS cyber-attacks.

The MOSAICS JCTD has several key deliverables that include development of an integrated, tested, and real-world proven MOSAICS tool suite to accomplish the ICS security identified previously. Key deliverables also include automated playbooks, development of a MOSAICS Concept of Operations (CONOPS), and updating the U.S. Cyber Command Advanced Cyber Industrial Control System TTPs (ACI TTP) for DOD, and industry training and implementation for the MOSAICS system. This will include a control system cyber baselining tool for ready implementation into all types of ICS to assess current ICS system vulnerabilities. As MOSAICS development and deployment advances, emerging spiral spinoffs are anticipated to better service user organizations for enhanced MOSAICS capabilities. Another key deliverable is the development of the Facilities-Related Control System (FRCS) design guide and updated DOD FRCS Unified Facilities Criteria (UFC 4-010-06) for integration into all DOD facilities and public works using a framework-based concept of employment.

The MOSAICS JCTD is meeting milestones and the MOSAICS team is creatively anticipating and overcoming obstacles as they are identified. In late FY20, the MOSAICS team will conduct a hardware-in-the-loop test on a state-of-the-art testbed under a simulated operational military exercise environment as a precursor to the final push to a fielded MOSAICS prototype. In August 2021, the Military Utility Assessment (MUA) is scheduled in advance of installation of the first fielded MOSAICS prototype. In late FY21, the first fielded MOSAICS prototype will be operational, and in the following year, transition will be underway to install MOSAICS at multiple locations with developed TTPs for full operator implementation. In the , the U.S. Navy shore installations are slated to lead the way with MOSAICS deployments programmed from FY22-25. Industry transition will follow via standards and regulatory organizations, to include the primary energy regulatory agencies, associations, institutes, corporations, and commissions, dependent on the specific requirements of the organization.

7.4 Summary

The NORAD and USNORTHCOM Commander told the House Armed Services Committee that "Our adversaries have watched, learned, and invested to offset our strengths while exploiting our weaknesses…they have demonstrated patterns of behavior that indicate their capability, capacity, and intent to hold our homeland at risk below the nuclear threshold [96]." That has forced NORAD and USNORTHCOM to reinvent its warfighter mindset and cultivate a homeland defense culture through network expansion and destruction of organizational silos of stove-piped information and capabilities. The capability demonstrated during the MOSAICS JCTD counters threats across all combatant commands and AORs within the and the private sector to ensure our ability to globally integrate the defense enterprise and dynamically source military capability worldwide.

CDRUSNORTHCOM also told the House committee, "We cannot defend the nation against 21st century threats with 20th century technology [96]." The MOSAICS JCTD is one component of the NORAD and USNORTHCOM technology transformation that fits perfectly into the overarching homeland JADC2 capability. MOSAICS will evolve into a critical element of the NORAD and

USNORTHCOM SHIELD, reaching across all AORs to counter the threat of a resurgent Russia, an assertive China, North Korea, Iran, natural disasters, Arctic development, CBRN threats, transnational networks, space, and cyber security.

8

Digital Transformation of Cyber-Physical Systems and Control Systems

Digital transformation has arrived in the Cyber-Physical Systems and Control Systems (CPS/CS) environments. As the access to the IIOT and discussion about cybersecurity and CIP for homeland defense expands, so does the opportunity for applying transformational capability for a variety of secure automation applications in CPS/CS. Drivers include the increased flexibility and ease of use for operators, scalability, modularity, greater memory access, evolving features such as wireless connectivity, and faster speed solutions. If the digital transformation hasn't touched an aspect of CPS/CS yet, it soon likely will. The digital transformation of CPS/CS results from a technology convergence trend affecting ICS during the past decade. The role of industrial controls to control machinery is changing as increased software, information, and communication technology increase these machines' possibilities. This change is ushering CPS/CS into a new era that will profoundly affect the security posture of mission-critical infrastructure.

The digital transformation of CPS/CS occurring now is very similar to the digital transformation of IT that that has taken place over the previous 50 years. Disrupters to the IT industry included the rise of the Electronic Manufacturing Services (EMS) industry, which led to the commoditization of IT components, Cloud computing, SOAR, and SDN. Government-led initiatives such as the MOSAICS JCTD are influencing an entire digital transformation of the OT space to leapfrog beyond the current capability with expanded use of software in the value chain. The MOSAICS JCTD is an example of a breadth of collaboration between the DOD, DOE, National Laboratories, University Affiliated Research Center (UARC), and private industry [97]. MOSAICS will demonstrate new capability within three years, with less than $20 million invested advancing the possibilities to the point that took more than 50 years

to achieve on the IT timeline in similar investment, research, development, experience, and commercial industry influence. A significant way to think of the digital transformation of CPS/CS is to think in terms of "function and effect" rather than unique, proprietary technology. This way of thinking is how new capabilities such as SOAR or SDN can be applied to machinery control [98].

8.1 Information Technology/Operational Technology Marketshare

Revenue in the CPS/CS industry today is still primarily generated from hardware sales. In contrast, this is very similar to where the IT industry market space was in the 1980s and early 1990s before the rise of the global EMS industry (see Figure 8-1). As OT converges on the same path as IT the functions and effects will drive the speed of adopting disruptive capabilities in the CPS/CS environments. For example, the global IT digital transformation market is expected to be worth $3,294 Billion by 2025 with an expected Compounded Annual Growth Rate (CAGR) of 22.7 percent [99]. The growth in the market is mainly attributed to the manufacturing industry. Sectors such as power utility, water, and building facilities are yet to be factored into this growth trajectory. In contrast, the global CIP market size is projected to grow to $153.3 Billion by 2025, with a CAGR of 3.4 percent [100]. Companies that get in front of these changes introduced by the digital transformation of CPS/CS stand to gain tremendously by the new market share. The parallel to the IT industry is worth observing.

8.1.1 Electronic Manufacturing Services Industry Commoditization

Taking a look back in time, the rise of the EMS industry played a large part in the IT industry's commoditization. Initially, some Original Equipment Manufacturers (OEMs) outsourced parts and components to contract manufacturing companies. These contract manufacturers specialized in fabricating a wide range of items for the OEMs. The industry took off in the 1990s when EMS companies offered expanded business models that essentially led to the complete manufacture of customer specifications through full lifecycle management (i.e., from design, test, integration, and assembly, logistics, to customer support). EMS changed the way IT was designed and mainly led to the commoditization of IT components. From the 1980s through 2000, the IT industry primarily focused on inventory and asset management, configuration management and defense, and identity capability.

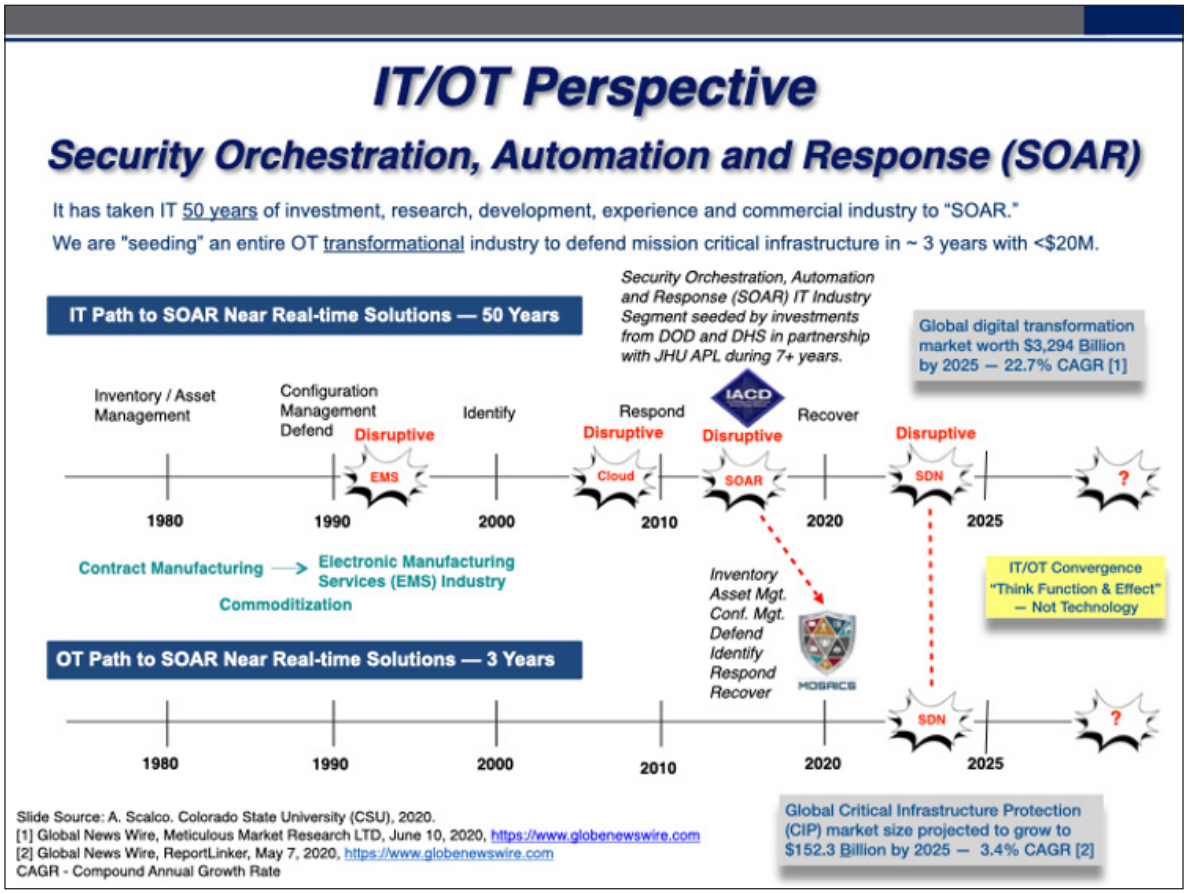

Figure 8-1. IT/OT Perspective and the Path to Security, Orchestration, Automation, and Response (Source: Authors).

8.1.2 Cloud Computing

Adoption of the Cloud was another huge digital transformational step in the IT industry. While the original idea of cloud-based data can be traced much earlier to the 1950s and 1960s, the benefits of ubiquitous cloud computing started to be fully realized in the early 2010 timeframe. By contrast, along the same timeline, OT was largely still considered to be "air-gapped," a network physical isolation state from unsecured networks such as the Internet and LANs, this would soon be proven to be a misnomer as a result of the world's first publicly known malware attack to "ICS" security, Stuxnet, in 2010 [101]. The malicious cyber-actor targeting OT that manage machines demonstrated that significant cyber events that could happen to IT enterprises could also occur to OT. Ongoing cyber-espionage campaigns targeting enterprise systems were now open to dangerous exploitations in CPS/CS. The important takeaway from Stuxnet was that the ability to detect and recover from a cyber-attack is as essential to OT as it is to IT enterprise networks. The technology convergence caused by the innovative capabilities of the IIOT highlighted what would become a trend and what would require greater attention to protect CPS/CS. From this point forward, operators of CI would have to defend assets from new vulnerabilities, which require advanced tools, knowledge, skills, and capabilities. In the decades that followed the concept of "cloud" computing, virtual private networks (VPNs) moved into the IT market space. Even

EMS companies offered to connect customers directly to the shop floor as technology become more affordable. Software as a Service (SaaS) gained access via the online IT market to data. It seemed everyone working in IT was accessing the cloud and launching new services using cloud technology. IT/OT seemed to be on parallel paths, yet philosophically different. Enter Secure Orchestration, Automation, and Response (SOAR) capability.

8.1.3 Secure Orchestration Automation and Response

SOAR was a term coined by Gartner Research for a capability developed by Johns Hopkins Applied Physics Laboratory (APL) through advanced research efforts sponsored by the DHS and the National Security Agency (NSA) called "Integrated Adaptive Cyber Defense." Using the IACD framework, SOAR solutions gather data from integrated software solutions and tools into a single pane for cybersecurity automation, orchestration, and information sharing using preapproved and designed "playbook" responses. APL recently announced it was teaming with the DHS's CISA to help state and local governments enhance their defenses by applying SOAR [102]. According to APL's press release, "The effort stems from recent APL research and pilot programs with critical infrastructure industries that showed how automated information sharing can shore up cyber defenses by reducing response time [102]." SOAR is a component of the capabilities that the MOSAICS JCTD will demonstrate to the DOD in July 2021 during a Military Utility Assessment (MUA). The MOSAICS demonstration could quickly serve as a model for CPS/CS cyber defensive capabilities. The SOAR capability introduces automation to improve networks' security and alleviate manual processes operators rely on today. SOAR brings IT and OT capability closer to respond and recover in near real-time. Enter the Software-Defined Networking (SDN) capability.

8.1.4 Software-Defined Networking

SDN provides the capability to change a network using software to control the network's behavior from a logically centralized system. This capability enables network operators to evolve network capabilities and manage networks even after they are deployed. SDN makes network management that was previously complicated, simpler, and more flexible. SDN appears to be the next industry disruption after SOAR capabilities (see Figure 3). SDN technology changes the way CPS/CS operations can be managed regardless of how complicated the network is an IT or OT. As new technology and methodologies are explored for CPS/CS, SDN will likely be incorporated into CPS/CS environments. SOAR automation of preapproved playbook responses is a path leading to developing the necessary knowledge, skills, and attributes of operators using transformational technology in the digital transition of CPS/CS.

8.2 Summary

Interface to the Internet creates a radical shift, and the corresponding need to rethink how cybersecurity principals and techniques are applied to CPS/CS environments. The DOD articulated the urgent need for defensive capabilities of CPS/CS for mission assurance of CI. The MOSAICS JCTD is the first demonstration of operational capability to enhance the security of CPS/CS [95]. The government and commercial industry require up to date, available, agile, and more cost-effective solutions to protect data. Billions of dollars are at risk every year from the economy due to cyber-attacks. Traditional government security solutions can take many years to develop, certify, and field. In many cases, these

solutions are just commercial versions of government solutions. By the time these capabilities are fielded, they can be outdated or obsolete technology. Digital transformation has arrived in the CPS/CS environments. MOSAICS is demonstrating the opportunity to realize transformational capability for various secure automation applications in CPS/CS. Drivers include the increased flexibility and ease of use for operators, scalability, modularity, greater memory access, evolving features such as wireless connectivity, and faster speed solutions.

The next capabilities on the near horizon are the applications provided by SDN, and other innovative, new technologies and methods. The Naval Facilities Engineering Systems Command (NAVFAC) is the leading the transition of MOSAICS capabilities to operational use. NAVFAC will integrate MOSAICS into operations and continue to lead the development and promotion of new ideas and innovative capabilities at the NAVFAC and Expeditionary Warfare Center (EXWC) to meet the Navy's mission objectives. The digital transformation that has taken the IT industry more than 50 years to realize is barreling toward the CPS/CS sectors (e.g., power, water, facilities). The centralized control system will make it easier to respond and recover from cyber events but will also require further research to understand better the impacts of the digital transition of CPS/CS. Additional research studies about the professionals in both IT and OT are needed to understand better and assess if the skill sets are available to handle the transition of these transformative capabilities in near-real time [103].

9

Deception Security for Internet of Things in Critical Infrastructure

IoT remains one of the most vulnerable components of CI due to the vast number of expected interconnected devices and their relatively low-cost designs needed to maintain competitiveness. It is evident that the need for cost-constrained IoT has created a challenge for secure and privacy-safe products. Many small manufacturers have entered this emerging technology without the resources available to define and follow a structured approach for security measures. Many companies prioritize product delivery of intended functions rather than security. Furthermore, in situations where minimal security features have been addressed, such as rudimentary authentication username and password procedures, the operational aspects of security, which include certificate management and the ability to systematically handle software upgrades, remain inadequate. Proprietary or non-standard offerings of IoT also add complexity since it is difficult to assess the security without wide access and open technical specifications for testing by experts. The closed nature of the design may inhibit the security community in guiding vendors or announcing the vulnerabilities in designs and to propose stronger protection.

The concept of IoT is not a new phenomenon. IoT enables sensors and other endpoint applications with communications back to a central processing station. Subsets of these devices have limited processing, bandwidth, and power capabilities, while other IoT devices connect to the Internet in ways similar to typical computers. This brings about challenges as the traditional approach to commonplace Internet security needs to be extended for IoT protocols. The security threat is exacerbated as malicious actors attempt to gain access to rich targets, usually in a stealthy manner, knowing that IoT still has significant vulnerabilities [104].

A failure to address these security concerns may potentially leave CI in a precarious state. Fortunately, security advancements have accelerated for IoT, including defensive deception strategies which have been demonstrated to improve the cybersecurity posture. Deception techniques make it more difficult for attackers to breach the true active IoT sensors/endpoints if a favorable ratio of decoys exceeding the number of working devices is implemented correctly. Further, extracting the detailed trail of intrusion from the decoy traps is used to enhance protection of the entire IoT system, along with possible attributions of the attacker. The use of replica deception techniques improves the security of critical and defense network infrastructure, especially as IoT devices become ubiquitous for various applications.

9.1 Attacker Steps Anticipated (Intrusion Kill Chain)

Attacks can originate in many forms, but the majority of exploits target application endpoints, such as IoT devices first, and then tend to move laterally to the sensitive elements of the network where critical information or assets are threatened. Attackers attempt to attain credentials so that a compromised IoT endpoint can be used as a launch to spread to other devices and network elements. Once breached, attacks can be of the form of eavesdropping, altering of data, denial of service, and other forms of malevolence. For IoT, the issue of overall safety, in addition to security, becomes paramount as the attacker may have more radical motives.

Of particular importance is the fact that CI is evolving whereby IoT endpoints can either connect through a direct path to a gateway or ad hoc through a wireless mesh using other IoT endpoints as transmission repeaters in the network. This later configuration complicates the security landscape and makes a defensive security posture more challenging. Further, an added dimension of complexity associated with proprietary protocols includes determining the trustworthiness of the selected vendor for security and physical protection of the devices [105].

With IoT security requirements, a perception often arises relating to intricacy required as compared to conventionally securing PCs (personal computers) and network security. IoT is in use today across some of the most critical industries. An additional pillar of "safety" needs to be considered as concerns become more apparent, especially when defending against attacks with extreme intent. Energy and smart grids, connected vehicles for transportation, manufacturing, human wearable devices/human implants, require a higher degree of scrutiny when it comes to designing for physical safety and minimizing the level of risk/impact should an exploit occur.

It is important to understand the model scenario of attack as defined in the cybersecurity community. Studies in the past have led to frameworks, such as the Intrusion Kill Chain developed from military/government-related initiatives and refined by researchers at Lockheed Martin Corporation [106]. Phases in the intrusion kill chain include reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objective. Figure 9-1 summarizes the phases and how it relates to attack effort.

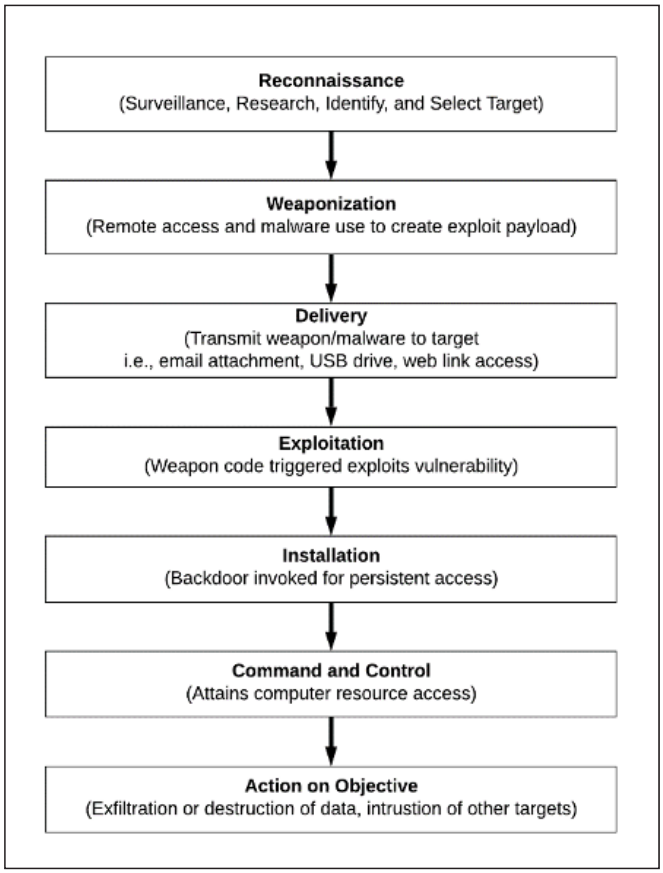

Figure 9-1. Intrusion Kill Chain – Representative Model (Source: Authors).

The progression of attack steps illustrates the importance of defensive initiatives early on in the sequence, especially before weaponization and delivery tactics are implemented. Defensive models should prioritize initiatives to proactively address all known threats, plugging identified vulnerabilities, and preparing for further attacker initiatives that will surely encompass further discovery of the attack plane. The reconnaissance phase, therefore, is an important area where defensive actions are valuable. Deception tactics in this regard play an important role.

Reconnaissance is the earliest stage in the attack cycle. Attackers survey the landscape, in this case the network resources of interest, and prepare to take further action. Attack methods are based on the information gathered during reconnaissance. It should be noted that at this early stage, it is advantageous to trick the attacker so that further malicious progress may be avoided. Deceptive technologies are able to not only fool, but also annoy the attacker by obfuscating the environment of interest. Early defensive actions are defined as proactive detection and mitigation. This set of initiatives is suited for early kill chain actions - reconnaissance, weaponization, and delivery. However, once the exploitation occurs, and continues through to action on objective stage, reactive containment and incident response initiatives must take place to return the network environment to a stable and cleansed state.

One important tenet for a successful IoT deceptive system is to make sure that attackers do not identify the decoys. The implementation should replicate the real environment without deviations of authentic device fingerprints that would alert an attacker. A successful deployment must be scalable,

while also able to be managed, provide reports, and take defensive actions. The solution must be scaled with minimum overhead as this will avoid performance issues, especially for IoT devices configured with low processing capacity and low bandwidth. The ultimate objective is to counteract with improved protection through actionable information conveyed about the intruder.

Use of deception technology becomes a valuable approach when industry and government seek to either catch the cybercriminal or, at the very minimum, deter the attacker. This is related to the "broken windows" analogy whereby attackers will continue to trespass and commit cyber exploits so long as others continue to perform similar activity without being caught or traced. Deception to confuse the intruders and block "broken window" entry would provide a more level playing field as a defense; at the same time, it would influence attackers to think twice as to overall repercussions, knowing that chances of being caught are now higher.

9.2 Honeypots and Honeynets

A common approach to gathering information about an intrusion is with the use of honeypots. Implementations of this type use bait to attract the attacker and can include credentials or file paths that appear intriguing, although they are altered representation of critical data [107]. In the simplest form, deception can be a single decoy honeypot as shown in Figure 9-2.

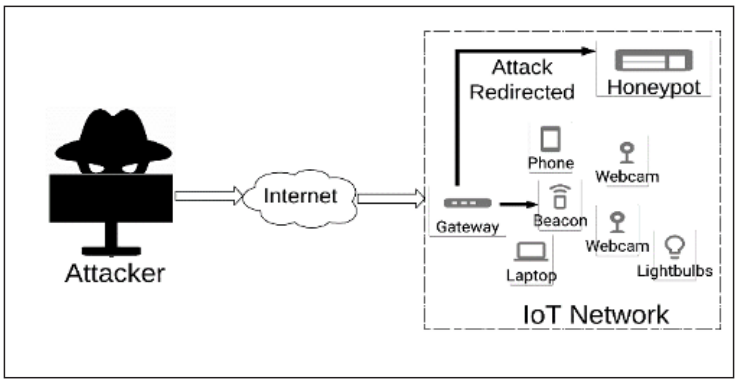

Figure 9-2. Simple Perspective on Attack Redirected to Honeypot (Source: Authors).

There are different methods and various levels of sensitivity for determining whether the data traffic entering the network is suspicious or expected [108]. Some implementations use unassigned IP address ranges that are being scanned or attempted by an attacker, indicating suspicious activity. Other triggers may be a port request or unsuccessful logins to critical servers. In such cases, the suspicious connection will be directed to the honeypot. The prevalence and attractiveness of honeypots is their simplicity to install and investigate the specific activity.

However, there are disadvantages to honeypot implementations. It is often assumed that the attacker is not expecting to encounter a honeypot, but this assumption is naïve. Research relating game theory in this area has shown that honeypots become less effective over the lifecycle of attacks as intruders improve disguise tactics to blend in with normal expected network traffic [109].

Advancing the IoT honeypot solution one step further, a network that provides greater interaction with several interconnected honeypots can be used. Whereas a honeypot may be one decoy, the investigative capabilities can be advanced with honeynets, essentially a network of honeypots that encourage further interaction with the activities of the intruder. The advantage here is that the honeynet

can provide additional insight into the mode of attack and the intent. Honeynets direct the suspicious activity to various forms of decoys, whether it is an improvised Windows or Linux operating system or a deceptive set of servers [110]. The disadvantage, in general, is the scalability limitations, along with cost and complications associated with such implementations. Honeynets are constructed based on what the organization believes will attract the intruder. If anything looks abnormal, the attacker will most likely abort.

9.3 Canary and Deception

So far, the description of deception has focused on redirecting the connection to confuse the attacker and gain attribution of the motive. A similar approach, called canary, can be an overlay within servers and file systems to replicate or provide fake content for attacker access. Canary file deception has been around for several years. Today, some providers of next-generation antivirus protection services have added canary files to endpoints to enhance their investigation and response efforts.

Canary tokens, often referred to as honey tokens, are deception at the content level within files, documents, or web pages to provide additional information. Canary tokens provide unique identifiers and may be implemented as alerts to notify defenders of resources being accessed. Alerts are similar to an email acknowledgment message that a sender receives upon the contents of a mail message being opened [111]. The use of canary tokens requires minimum overhead and is well suited for transmission over bandwidth-limited networks. Figure 9-3 depicts a simple view of a canary approach.

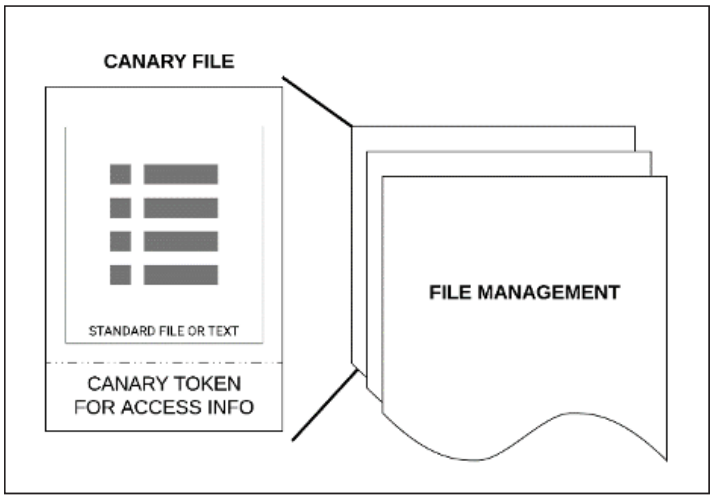

Figure 9-3. Canary file with token appended for tracking (Source: Authors).

Canary tokens can be leveraged in the IoT realm to alert on tampered endpoints to the centralized monitoring or control system. It is well known that such tokens provide valuable cyber attribution to plug the broken windows and/or trace back to the intruder.

Canary implementation can also be used for malicious purposes and retaliation. In such cases, read filters and logging can further identify the motif of the intrusion and add countermeasures, including phone-home trackers which can be embedded. However, this often tests the limits of what can be conducted legally as part of retaliation, or understanding the attack and its goals.

9.4 Use of Proxy and Non-Default Configurations

If extra steps are taken to mask standard networking and port configurations, the obscurity makes the intruder's reconnaissance and attack delivery more difficult. Deploying defensive tactics delay an exploit, therefore becoming favorable for the security actions of the system.

Instead of using standard port numbers, a defensive strategy would be to alter port configurations. For example, if Server Message Block (SMB) is not configured with the default port 445 and instead the network administrator monitors port 445 for attacks, information of malicious intent and intrusion can be captured. Configuring away from default settings is a recommended method in many network scenarios to obscure the landscape [112]. As another illustration, Remote Desktop Protocol (RDP) connections are commonly used for attacks on default port 3389. Changing the port number and other network configurations away from default settings makes the attacker work harder to determine the correct topology to be successful in its malintent. This defensive use of obscurity is not a way to secure CI but is intended to frustrate and delay the attackers' efforts.

9.5 Ubiquitous Deception

This brings up recent approaches that use deception techniques with the objective of entangling intruders as opposed to attracting them once in the network [113]. In other words, implementations are deployed with proportional decoys throughout the environment so that the probabilistic outcome would be extremely low for the attacker to have succeeded in reaching authentic IoT endpoints altogether. Solutions in this regard have progressed to include enriched deception by being widely distributed and being capable of stealthy interactions with a better determination of the attacker's intent and approach.

As an attacker takes action and attempts to make lateral moves to other endpoints, alerts are sent, and deception is activated. At this point, decoys can be multiples of the real system resulting in a perceived larger number of devices than actually in use. The attacker's attempt is directed to a trap server instead of the real assets that were targeted. With numerous deceptions invoked, the likelihood is significant that the intruder makes an incorrect decision and does not realize it. This compels the attacker to perform more work and leave more trails, positive characteristics for an investigation aligned with a defensive strategy.

The deceptive elements are typically maintained in the virtual server(s) that spread the decoys across each family class of protection defined. The information attained from real-time forensics of the trap logs can be channeled to the management console for countermeasures. Figure 9-4 depicts a generic representation of a deception solution as it relates to IoT.

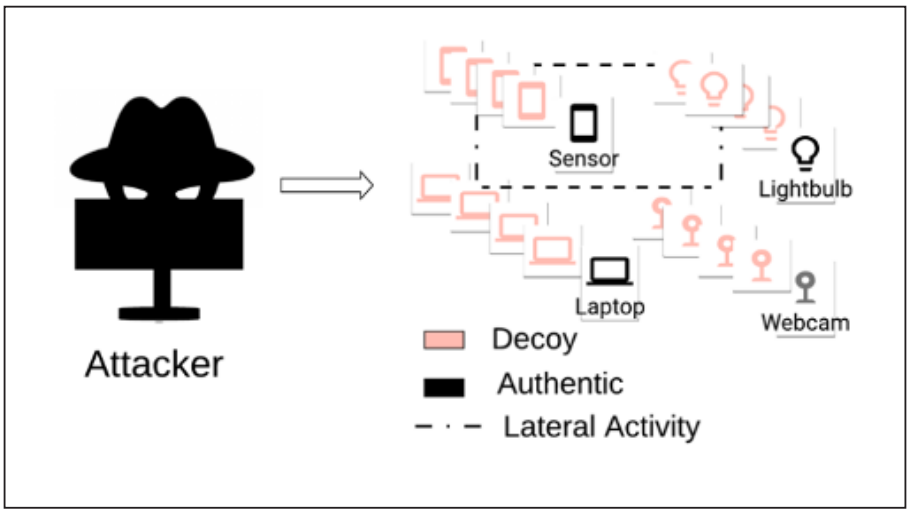

Figure 9-4. Deceptive View from Attacker Perspective (Source: Authors).

Significant differences between honeypot/honeynet architectures compared to obfuscation solutions provide impetus to advance the technology as part of overall defenses of IoT security. Some of these characteristics are:

- ***Entanglement:*** Honeypot and honeynets are normally used to lure attackers to an investigation area. On the other hand, deception deploying replications of authentic devices can entangle or mislead attackers so the probability of connecting with the real device is extremely low.
- ***Authenticity vs. Imitation:*** With ubiquitous deception, however, the families of applications defined for this solution obscures the network elements, making the attacker unaware of whether it is real or deceptive. Further, advanced deception is often orchestrated to be dynamic as the endpoint characteristics change over time. This prevents the intruder from using previously harvested information to build out their exploit tactics.
- ***Scalability:*** Increasing the number of honeypots could be costly and resource-intensive. Ubiquitous deception approaches can be deployed across the entire network without the need for software (agents) on authentic devices. Instead, virtual instances of the devices are created and replicated through the network.
- ***Veracity of Alerts:*** Elimination of false alerts is improved with deception technology as opposed to honeypots. With honeypots residing in the network, legitimate endpoints may encounter and interact accidentally, triggering a false intrusion. This raises the level of false-positive conditions that a Security Operation Center may need to deal with as part of alarm fatigue.

9.6 Attack Analysis and Countermeasures

Detecting and containing breaches can take a long time. Recent studies indicate that the average time it takes for an organization to detect a data breach was 197 days [114]. Further, it took more than 30 days to contain the breach once it was identified [114]. Expediting response time is needed so that attackers do not seek to gain continuous critical information, often by moving laterally across the network.

With deception technology, an attacker can continue to communicate with decoys so that a prompt response can be taken. An improvement would be accompanied by continued monitoring of the attacker tracks to determine other protective measures as they are divulged to the deceptive devices and traps monitoring the malicious actions. The challenge here is that sophisticated attackers often try to purge their trails as soon as the objectives are met. It is important for logs to remain unaltered and protected against such activity.

An important takeaway about deploying deception technology is to understand the motives and tactics of the attacker. With advanced deception practices applied to be specifically formulated for the implementer's network, a more realistic assessment can be attained, tailored to the environment under attack. In this regard, the analysis does not rely as heavily on potentially outdated threat intelligence or information that may be less meaningful than the intelligence discovered as part of deception at the target site.

9.7 Countermeasures One Step Further

In addition to improving the defense posture, counterattacks could be conducted. Defensive organizations can use deception technology to leverage the information about attacks to perform their own offensive response. At this point, it is not recommended that commercial organizations implement offensive neutralization. Instead, the information gathered from the attack be communicated to the authorities so that proper enforcement can be taken.

Law enforcement and military can take a variety of countermeasures, some of which are based on the deceptive implementation discussed above. For instance, the canary token concept can be extended one step further with decoy executables (.exe) and trap applications, including file name examples (such as vpnconfig.exe or sysprep.exe) to bait the intruder. Adding a token canary to the executable will alert the implementer, and also may be used to implement a backdoor that could be used by government to ultimately derive the identification or location of the intruder, i.e., deploying a beacon (ping) that would derive where the executable was being requested or where it was activated.

The attacker's trail of activity can be of significant value to the security community. As far as government is concerned, authorities approved with handling countermeasures may be able to dispatch special reconnaissance, although the attackers may be sophisticated and difficult to track down.

9.8 Internet of Things Endpoint Considerations

Deceptive solutions addressing the IoT environment have additional hurdles when compared to traditional networks responsible for the security of computers, such as in a corporate setting. As mentioned earlier, IoT may be limited with respect to processing capacity, especially if connected via a bandwidth-constrained wireless network (i.e., ZigBee, Bluetooth, 802.15.4e standards). As such, it is important to limit the amount of traffic and interactions in a narrowed communications channel to avoid overload and to prevent operational degradation.

Second, obfuscating IoT endpoints must replicate the same protocol interaction across the decoys as they are for the true endpoints. It is important to note that the exchanges for messaging leave

patterns that may become evident to the intruder. The difference in protocols relate to cases where IoT devices are deployed in wireless networks and/or have bandwidth constraints, limited power and communications range. In such cases a shim protocol called 6LoWPAN is used to manage the compression and interoperability of the communications traffic across a constrained IoT domain [115].

Many IoT deployments involve communications from the endpoint to a controller. Often, this involves a gateway to pass traffic between the IoT device and the gateway element. Setting up decoys with accurate messaging protocol in use becomes important in the implementation of deception for the IoT environment. Here, protocol conversions may take place at a gateway, often passing through several network elements. Eavesdropping or data spoofing may become possible should the underlying security of these elements, and connections become susceptible to man-in-the-middle attacks.

Finally, the diversity of IoT devices, whether endpoints are sensors, actuators, surveillance devices, or other appliances, makes the deception architecture more involved compared to standard enterprise networks used primarily for computers, servers, printers, and network equipment. IoT, by its very definition, can be any type of device that has a network connection. Implementation of IoT applications generally involve a controller (control system), sensors, actuators, and possibly a web interface for user information retrieval or settings. Therefore, the replication must not have identical fingerprints to make the architecture effective and not divulge any attribute that will inform the intruder that defensive deception is in place. Because of the numerous elements associated with IoT the vulnerabilities can be wide and severe.

9.9 Summary

IoT deception plays an important countermeasure role for Homeland Defense and DOD cybersecurity initiatives as it offers enhanced options to identify, isolate, and respond to threats in our change to CI capabilities to funnel data and evidence from defensive deception technology have been shown to improve overall protection for the IoT ecosystem in conjunction with improved regulations, enforcement, and counter responses.

The use of deception for IoT CI has been limited to date and instead has been considered mostly in the larger context of overall computer security. There are additional requirements to make deception work for IoT, especially with the diversity of protocols and types of applications in use, many of which differ from conventional computers. Further deployments of deception IoT strategies should be considered to improve the overall cybersecurity posture of all U.S. CI.

10

Conclusion

Today CIP involves not only the protection of physical assets from a range of natural and manmade threats, but also the protection of the cyber systems that often provide the backbone of CI. Adding to the protection challenge is the increasing complexity resulting from the interconnectivity of many infrastructure elements as a result of IoT and other technological advances. Advancements in AI, big data utilization, and predictive analytics greatly benefit and strengthen CIP efforts.

At the national level, various strategic documents, including the *National Security Strategy of the United States and the National Defense Strategy,* outline the federal government's responsibility to protect the American people, which includes protecting CI, and points out that the operational environment includes the homeland. In particular, the National Security Strategy asserts that "will protect our critical infrastructure and go after malicious cyber actors [116]." Numerous organizations throughout the national level of government have responsibility for CIP.

Within DHS, the Cybersecurity & Infrastructure Security Agency has overall responsibility for ensuring the security and resiliency of the nation's CI and leads the national response for protecting CI through the NIPP and the 16 CI Sector-Specific Plans. Working with partners across the public and private sectors, CISA operates the National Risk Management Center (NRMC) as a planning, analysis, and collaboration center to identify and address the most significant risks to our nation's CI. This includes working with the other government organizations that are designated as the SSA for various CI sectors, and the private sector that owns and operates the vast majority of the nation's CI.

The DOD contributes to the efforts at the national level with its Defense Critical Infrastructure Program (DCIP), and with each of the services addressing CI protection in various policies and

strategies. For example, in its Installations Strategy, the Army recognizes that "installations are no longer sanctuaries," and "anticipates that adversaries will use sophisticated intelligence, surveillance, and reconnaissance (ISR) networks to target both military installations and soft targets… including … civilian infrastructure [117]." The DOD is also the designated SSA for the DIB sector, the companies that design, produce, deliver, and maintain all materiel to meet U.S. military requirements.

At the state level, each of the 55 states, territories, and federal district develop and execute plans for the protection of their CI. Each has emergency management departments that among other activities prepares for disasters and other events that can impact CI, in order to protect the vital facilities within their areas of responsibility.

With the private sector owning the vast majority of the nation's CI, it has the vital role of implementing needed requirements to protect their assets. CISA works with the private sector via infrastructure sector partnerships to ensure an integrated approach to CIP. This includes the working with the owners of CI to mitigate risks and reduce threats from natural and manmade threats.

As the world has become evermore interconnected and reliant upon the Internet for day-to-day functions, a new front has opened in nation state competition. The ability for a near peer actor to cause disruption, harm, and inefficiency in areas formerly thought invulnerable is unprecedented. In turn, successful attacks on CI can sow mistrust and confusion in the population and adversely affect military readiness. Further, the challenges associated with attributing the source of such attacks complicates the problem, and ascertaining whether such an attack warrants a response (kinetic or non-kinetic) is an even more difficult matter. Setting aside the discussion of whether a particular incident crosses the threshold for casus belli, the difficulties in detecting, assessing, attributing, and responding to such attacks is a complex and difficult undertaking. That said, it is unlikely that the U.S. will go "backward," and attempt to eliminate the distinct advantages presented by an IOT; therefore, it is necessary to assess vulnerabilities and work cooperatively to address these areas. The public-private relationship is cemented in all the CI sectors, and together, they have a wealth of cyber capabilities. These resources must be properly organized, harnessed, and focused in order to prevent cyber attacks against the lifeblood of the U.S., its critical infrastructure.

The nation's CI facilities and resources are vast, and protecting it all is a vital mission. Protecting the nation's CI requires the efforts of every level of government, as well as the businesses that operate them. These assets provide essential services that support the American society, drive the U.S. economy, and contribute to the American way of life.

Abbreviations and Acronyms

AB ..... Air Break
ACI ..... Advanced Cyber Industrial
AI ..... Artificial Intelligence
BIM ..... Building Information Model
CBRN ..... Chemical, Biological, Radiological, and Nuclear
CI ..... Critical Infrastructure
CIP ..... Critical Infrastructure Protection
CISA ..... Cybersecurity & Infrastructure Security Agency
CM ..... Configuration Management
CONUS ..... Continental United States
COTS ..... Commercial off the Shelf
CPS ..... Cyber-Physical System
CS ..... Control System
CWA ..... Clean Water Act
DHS ..... Department of Homeland Security
DIB ..... Defense Industrial Base
DOD ..... Department of Defense
DOE ..... Department of Energy
DSCA ..... Defense Support of Civil Authorities
DSRC ..... Distributed System Research Consortium
DTIC ..... Defense Technical Information Center
EMS ..... Electronic Manufacturing Services
EPA ..... Environment Protection Agency
ESF ..... Emergency Support Function
EXWC ..... Expeditionary Warfare Center
FEMA ..... Federal Emergency Management Agency
FRCS ..... Facility Related Control System
GAO ..... Government Accountability Office
GOTS ..... Government off the Shelf
GPS ..... Global Positioning System
HAZMAT ..... Hazardous Material

HDIAC ..... Homeland Defense & Security Information Analysis Center
HMI ..... Human-Machine Interface
HVAC ..... Heating, Ventilation, and Air Conditioning
IACD ..... Integrated Adaptive Cyber Defense
ICS ..... Industrial Control System
IDT ..... Intrusion Detection System
IIoT ..... Industrial Internet of Things
INL ..... Idaho National Laboratory
IP ..... Internet Protocol
IoT ..... Internet of Things
IT ..... Information Technology
JCTD ..... Joint Capability Technology Demonstration
JHU APL ..... Johns Hopkins University Applied Physics Laboratory
JIOR ..... Joint Information Operations Range
KSA ..... Knowledge, Skill, and Attribute
LAN ..... Local Area Network
MOSAICS ..... More Situational Awareness for Industrial Control Systems
MUA ..... Military Utility Assessment
NAVFAC ..... Naval Facilities Engineering Systems Command
NIPP ..... National Infrastructure Protection Plan
NORAD ..... North American Aerospace Defense Command
NDS ..... National Defense Strategy
NHSRC ..... National Homeland Security Research Center
NRF ..... National Response Framework
OEM ..... Original Equipment Manufacturer
OT ..... Operational Technology
PC ..... Personal Computer
PCII ..... Protected Critical Infrastructure Information
PLC ..... Program Logic Controller
PNNL ..... Pacific Northwest National Laboratory
PPP ..... Public-Private Partnership

RA ..... Reference Architecture
RDP ..... Remote Desktop Protocol
RTU ..... Remote Terminal Unit
SaaS ..... Software as a Service
SAS ..... Substation Automation System
SCADA ..... Supervisory Control and Data Acquisition
SDN ..... Software-Defined Networking
SDWA ..... Safe Drinking Water Act
SHIELD ..... Strategic Home and Integrated Ecosystem for Layered Defense
SMB ..... Server Message Block
SOAR ..... Secure Orchestration, Automation, and Response
SOAR ..... State of the Art Report
SSA ..... Sector Specific Agency
TRL ..... Technology Readiness Level
TTP ..... Tactics, Techniques, and Procedures
UARC ..... University Affiliated Research Center
USACE ..... United States Army Corps of Engineers
USDA ..... United States Department of Agriculture
USINDOPACOM ..... United States Indo-Pacific Command
USNORTHCOM ..... United States Northern Command
UTM ..... Unified Threat Management
VLAN ..... Virtual Local Area Network
WAN ..... Wide Area Network

References

[1] Cybersecurity & Infrastructure Security Agency, "Infrastructure Security," Department of Homeland Security, [Online]. Available: https://www.cisa.gov/infrastructure-security. [Accessed 16 November 2020].

[2] W. J. Clinton, "PDD-63 - Critical Infrastructure Protection, 5/20/1998," 20 May 1998. [Online]. Available: https://clinton.presidentiallibraries.us/items/show/12762. [Accessed 16 November 2020].

[3] 107th Congress, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001," 26 October 2001. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf. [Accessed 16 November 2020].

[4] Cybersecurity & Infrastructure Security Agency, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," Department of Homeland Security, 17 December 2003. [Online]. Available: https://www.cisa.gov/homeland-security-presidential-directive-7. [Accessed 16 November 2020].

[5] B. Obama, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," The White House, 12 February 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Accessed 16 November 2020].

[6] Under Secretary of Defense for Policy, "Office of the Assistant Secretary of Defense for Homeland Defense and Global Security," Department of Defense, [Online]. Available: https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Global-Security/Defense-Critical-Infrastructure-Program/Roles/. [Accessed 16 November 2020].

[7] Cybersecurity and Infrastructure Security Agency, "Reducing National Risk," April 2019. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/19_0430_cisa_nrmc-reducing-national-risk.pdf. [Accessed 28 September 2020].

[8] Cybersecurity and Infrastructure Security Agency, "A Guide to Critical Infrastructure Security and Resilience," November 2019. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf. [Accessed 28 September 2020].

[9] P. Toth, NIST MEP cybersecurity self-assessment handbook for assessing NIST SP 800-171 security requirements in response to DFARS cybersecurity requirements, NIST HB 162, Gaithersburg, MD: National Institute of Standards and Technology, Nov. 2017.

[10] I. H. Sarker, A. Colman, J. Han, A. I. Khan, Y. B. Abushark, and K. Salah, "BehavDT: A Behavioral Decision Tree Learning to Build User-Centric Context-Aware Predictive Model," *Mob. Netw. Appl.*, vol. 25, no. 3, pp. 1151–1161, Jun. 2020, doi: 10.1007/s11036-019-01443-z.

[11] B. Van Niekerk and M. S. Maharaj, "Relevance of Information Warfare Models to Critical Infrastructure Protection," *Sci. Mil. - South Afr. J. Mil. Stud.*, vol. 39, no. 2, Nov. 2011, doi: 10/d9dskw.

[12] J. Mandelblatt, C. Schechter, D. Levy, A. Zauber, Y. Chang, and R. Etzioni, "Building Better Models: If We Build Them, Will Policy Makers Use Them? Toward Integrating Modeling into Health Care Decisions," *Med. Decis. Making*, vol. 32, no. 5, pp. 656–659, Sep. 2012, doi: 10/ghf4xx.

[13] A.-D. Huo, J. Dang, J.-X. Song, X. H. Chen, and H.-R. Mao, "Simulation modeling for water governance in basins based on surface water and groundwater," *Agric. Water Manag.*, vol. 174, pp. 22–29, Aug. 2016, doi: 10/f8w5gn.

[14] L. Morris, M. Mazarr, J. Hornung, S. Pezard, A. Binnendijk, and M. Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.* RAND Corporation, 2019.

[15] S. Skorobogatov and C. Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," in *Cryptographic Hardware and Embedded Systems – CHES 2012*, vol. 7428, E. Prouff and P. Schaumont, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 23–40.

[16] "New policy prohibits DoD employees from using GPS services in operational areas," *Defense Logistics Agency.* https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1597116/new-policy-prohibits-dod-employees-from-using-gps-services-in-operational-areas/ [Accessed Oct. 29, 2020].

[17] "New Policy Prohibits GPS Tracking in Deployed Settings," *U.S. Department of Defense.* https://www.defense.gov/Explore/News/Article/Article/1594486/new-policy-prohibits-gps-tracking-in-deployed-settings/ [Accessed Oct. 29, 2020].

[18] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits," in *2014 IEEE Security and Privacy Workshops*, San Jose, CA, May 2014, pp. 236–250, doi: 10/ghf4x3.

[19] A. Guzman, S. Ishida, E. Choi, and A. Aoyama, "Artificial intelligence improving safety and risk analysis: A comparative analysis for critical infrastructure," in *2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Dec. 2016, pp. 471–475, doi: 10/ghf4x4.

[20] "U.S. Critical Infrastructure Victim of Ransomware Attack," *CPO Magazine*, Mar. 05, 2020. https://www.cpomagazine.com/cyber-security/u-s-critical-infrastructure-victim-of-ransomware-attack/ [Accessed Oct. 29, 2020].

[21] "Significant Cyber Incidents | Center for Strategic and International Studies." https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed Oct. 29, 2020].

[22] "Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S." https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#11d3ec7142eb [Accessed Oct. 29, 2020].

[23] L. Jinghua and L. Jinghua, "What Are China's Cyber Capabilities and Intentions?," *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 [Accessed Oct. 29, 2020].

[24] "OT Cyberattack a Greater Concern than Enterprise Data Breach for 3 in 4 IT Security Professionals," *Claroty*. https://claroty.com/resource/ot-cyberattack-a-greater-concern-than-enterprise-data-breach-for-3-in-4-it-security-professionals/ [Accessed Oct. 29, 2020].

[25] "What is Social Engineering? Defining and Avoiding Common Social Engineering Threats," *Digital Guardian*, Jul. 06, 2015. https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats [Accessed Oct. 29, 2020].

[26] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced Social Engineering Attacks," Journal of Information Security and Applications, vol. 22, pp. 113-122, Jun. 2015.

[27] N. Y. Conteh and P. J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, Feb. 2016, doi: 10/ghg8ph.

[28] K. Shin, K. M. Kim, and J. Lee, "A Study on the Concept of Social Engineering Cyber Kill Chain for Social Engerneering based Cyber Operations" *Journal of The Korea Institute of Information Security & Cryptology*, vol. 28, no. 5, pp. 1247–1258, Oct. 2018, doi: 10/ghg8pm.

[29] J. Pollack and P. Ranganathan. (July-August 2018). Social Engineering and Its Impacts on Critical Infrastructure: A Comprehensive Survey. Presented at SAM '18. [Online]. Available: https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/SAM4036.pdf.

[30] G. Baryannis, S. Validi, S. Dani, and G. Antoniou, "Supply chain risk management and artificial intelligence: state of the art and future research directions," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2179–2202, Apr. 2019, doi: 10/ggjnmd.

[31] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 16–23, Jan. 2015, doi: 10/ghg8qs.

[32] O. Egbue, D. Naidu, and P. Peterson, "The role of microgrids in enhancing macrogrid resilience," in *2016 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, Oct. 2016, pp. 125–129, doi: 10/ghg8q4.

[33] Y. Zhou, Z. Md. Fadlullah, B. Mao, and N. Kato, "A Deep-Learning-Based Radio Resource Assignment Technique for 5G Ultra Dense Networks," *IEEE Netw.*, vol. 32, no. 6, pp. 28–34, Nov. 2018, doi: 10/ghg8q9.

[34] P. Miller, "What is edge computing?," *The Verge*, May 07, 2018. https://www.theverge.com/circuitbreaker/2018/5/7/17327584/edge-computing-cloud-google-microsoft-apple-amazon [Accessed Oct. 29, 2020].

[35] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018, doi: 10/ghg8rh.

[36] A. T. Murray, "Critical infrastructure protection: The vulnerability conundrum," *Telemat. Inform.*, p. 10, 2012, doi: 10/crnqbr.

[37] "Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf." Accessed: August 12, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

[38] Environmental Protection Agency, "Water and Wastewater Sector-Specific Plan," Department of Homeland Security, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. [Accessed on October 29, 2020].

[39] A. Klobuchar, "Text - S.3021 - 115th Congress (2017-2018): America's Water Infrastructure Act of 2018," Oct. 23, 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3021/text [Accessed July 15, 2020].

[40] Department of Homeland Security, "Dams Sector-Specific Plan," Department of Homeland Security, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf. [Accessed on October 29, 2020].

[41] Department of Homeland Security, "Communications Sector-Specific Plan," Department of Homeland Security, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf. [Accessed on October 29, 2020].

[42] J. Cornyn, "S.893 - 116th Congress (2019-2020): Secure 5G and Beyond Act of 2020," Mar. 23, 2020. https://www.congress.gov/bill/116th-congress/senate-bill/893 [Accessed Oct. 29, 2020].

[43] Department of Transportation, "Transportation Systems Sector-Specific Plan," Department of Homeland Security, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf. [Accessed on October 29, 2020].

[44] Department of Energy, "Energy Sector-Specific Plan," Department of Homeland Security, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. [Accessed on October 29, 2020].

[45] "Executive Order on Securing the United States Bulk-Power System," *The White House*. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/ [Accessed Oct. 29, 2020].

[46] Cybersecurity & Infrastructure Security Agency, "Sector-Specific Agencies," *Department of Homeland Security,* [Online]. Available: https://www.cisa.gov/sector-specific-agencies. [Accessed November 18, 2020].

[47] The Joint Staff, "Joint Publication 3-28, Defense Support of Civil Authorities," 29 October 2018. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf. [Accessed 29 October 2020].

[48] Office of the Undersecretary of Defense for Acquisition and Sustainment, and Office of the Deputy Assistant Secretary of Defense for Industrial Policy, "Assessing the Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018. [Online]. Available: https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF. [Accessed March 2, 2021].

[49] P. Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination," *Bull. At. Sci.*, vol. 74, no. 6, pp. 368–373, Nov. 2018, doi: 10/ghg8t8.

[50] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, Sep. 2011, pp. 1028–1031, doi: 10/b9vjqq.

[51] A. I. Voda and L. D. Radu, "Artificial Intelligence and the Future of Smart Cities," *BRAIN Broad Res. Artif. Intell. Neurosci.*, vol. 9, no. 2, Art. no. 2, May 2018.

[52] Cybersecurity & Infrastructure Security Agency, "Trust in Smart City Systems Report," Department of Homeland Security, [Online]. Available: https://www.cisa.gov/publication/trust-smart-city-systems-report. [Accessed on March 2, 2021].

[53] T. T. Neaves and J. J. Keifer, "Implementing Successful Strategies for Emergency Management and Homeland Security," Natl. Acad. Public Adm. Am. Soc. Public Adm., vol. Memos to Natoinal Leaders, 2016.

[54] T. E. Thornton, C. Murphy-Greene, and K. A. Simon, "Communal Resiliency and Environmental Justice Examining the Aftermath of the Deep Water Horizon Oil Spill," J. Emerg. Manag., Forthcoming.

[55] T. T. Neaves, T. A. Wachhaus, and G. A. Royer, "The Social Construction of Disasters in the United States: A Historical and Cultural Phenomenon," J. Emerg. Manag., vol. 15, no. 3, Art. no. 3, May 2017. doi: 10.5055/jem.2017.0326.

[56] T. Steinberg, Acts of God: The Unnatural History of Natural Disaster in America. Cary: Oxford University Press, 2000.

[57] P. L. Abbott, Natural disasters, 6th ed. Boston: McGraw-Hill, 2008.

[58] J. A. Bullock, G. D. Haddow, and D. P. Coppola, Introduction to Emergency Management. Butterworth-Heinemann, 2017.

[59] E. H. Oh, "Impact analysis of natural disasters on critical infrastructure, associated industries, and communities," Ph.D., Purdue University, United States -- Indiana, 2010.

[60] M. Lindell and C. Prater, "Introduction to Emergency Management," John Wiley Sons, 2007.

[61] B. Wisner, J. Adams, and World Health Organization, Eds., Environmental health in emergencies and disasters: a practical guide. Geneva: World Health Organization, 2002.

[62] "Executive Order on Securing the United States Bulk-Power System," The White House. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/ [Accessed Oct. 29, 2020].

[63] U. C. Bureau, "Coastline County Population Continues to Grow," The United States Census Bureau. https://www.census.gov/

library/stories/2018/08/coastal-county-population-rises.html [Accessed Oct. 02, 2020].

[64] "ICE Cases: Gulf War Aftermath." https://mandalaprojects.com/ice/ice-cases/kuwait.htm [Accessed Dec. 16, 2020].

[65] "The eight failures that caused the Gulf oil spill | New Scientist." https://www.newscientist.com/article/dn19425-the-eight-failures-that-caused-the-gulf-oil-spill/ [Accessed Dec. 16, 2020].

[66] "28 CFR § 0.85 - General functions.," LII / Legal Information Institute. https://www.law.cornell.edu/cfr/text/28/0.85 [Accessed Oct. 02, 2020].

[67] The National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," Government Printing Office. [Online]. Available: https://www.9-11commission.gov/report/911Report.pdf. [Accessed February 4, 2021].

[68] W. J. Petak, "Emergency Management: A Challenge for Public Administration," Public Adm. Rev., vol. 45, pp. 3–7, 1985, doi: 10/b62hfm.

[69] W. A. Wallace and F. De Balogh, "Decision Support Systems for Disaster Management," Public Adm. Rev., vol. 45, pp. 134–146, 1985. doi: 10/fjb5bm.

[70] J. Weichselgartner, "Disaster mitigation: the concept of vulnerability revisited," Disaster Prev. Manag., vol. 10, no. 2, pp. 85–95, 2001, doi: 10/fnsn59.

[71] D. Paton and D. Jackson, "Developing disaster management capability: an assessment centre approach," Disaster Prev. Manag., vol. 11, no. 2, pp. 115–122, 2002, doi: 10/b82f26.

[72] T. A. Birkland, Lessons of disaster policy change after catastrophic events. Washington, D.C: Georgetown University Press, 2006.

[73] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control Syst., vol. 21, no. 6, pp. 11–25, 2001, doi: 10/c7qpp9.

[74] P. Choate and S. Walter, America in Ruins: The Decaying Infrastructure. Durham, N.C.: Duke Press, 1981.

[75] W. M. Leavitt and J. J. Kiefer, "Infrastructure Interdependency and the Creation of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans," Public Works Manag. Policy, vol. 10, no. 4, pp. 306–314, Apr. 2006, doi: 10/cf5nkr.

[76] K. Dramowicz, "Geographic Dimensions in Data Mining," ESRI Bus. GeoInfo Summit, Apr. 2009.

[77] P. Cobb, "Competitive Intelligence through Data Mining," J. Compet. Intell. Manag., vol. 1, no. 3, 2003.

[78] K.-T. Chang, Introduction to Geographic Information Systems, Eighth edition. New York, NY: McGraw-Hill Education, 2016.

[79] D. Ingram and J. Ingram, "GIS for Thread Analysis," GeoIntelligence Mag., Dec. 2003.

[80] A. Haque, "GIS, Public Service, and the Issue of Democratic Governance," Public Adm. Rev., vol. 61, no. 3, pp. 259–265, 2001. doi: 10.1111/0033-3352.00028.

[81] M. Gascó, "New Technologies and Institutional Change in Public Administration," Soc. Sci. Comput. Rev., vol. 21, no. 1, pp. 6–14, 2003, doi: 10/cphcfd.

[82] S. Barnes and F. Sietzen Jr, "GeoIntelligence: a foundation for security?," Geospatial Solut., vol. 13, no. 11, p. 24, 2003.

[83] C. E. Unterberg and Towbin, "Informatics/Analytics Market," Chesap. Innov. Cent., vol. CEUT-CIV Security Insights Report, Nov. 2005.

[84] M. H. Moore, "Sizing up Comstat: an important administrative innovation in policy," Criminal. Public Policy, vol. 2, no. 3, pp. 469–494, 2003, doi: 10/c7h6k7.

[85] M. H. Moore and A. A. Braga, "Measuring and improving police performance: the lessons of Compstat and its progeny," Polic. Int. J. Police Strateg. Manag., vol. 26, no. 3, pp. 439–453, 2003, doi: 10/bssvj5.

[86] W. F. Walsh and G. F. Vito, "The Meaning of Compstat: Analysis and Response," J. Contemp. Crim. Justice, vol. 20, no. 1, pp. 51–69, 2004, doi: 10/frfkqf.

[87] J. R. Firman, "Deconstructing Comstat to clarify its intent," Criminal. Public Policy, vol. 2, no. 3, pp. 457–460, 2003, doi: 10/cgvxwd.

[88] T. E. Thornton, C. Murphy-Greene, and K. A. Simon, "Communal Resiliency and Environmental Justice Examining the Aftermath of the Deep Water Horizon Oil Spill," J. Emerg. Manag., Forthcoming.

[89] T. T. Neaves, D. Nelson, and R. D. Kauzlarich, "Communal Resiliency and Integrated Emergency Operations," Natl. Counc. Sci. Environ., vol. January 7-9, 2019.

[90] "Metal Demand for Renewable Electricity Generation in the Netherlands," Metabolic. https://www.metabolic.nl/publications/metal-demand-for-renewable-electricity-generation-in-the-netherlands-pdf/ [Accessed December 16, 2020].

[91] A. Hashmani, *Analysis of Substation Automation System Based on IEC 61850 Using Topical Software*, thesis, April 29, 2016.

[92] B. Lydon, "IEC 61850 Power Industry Communications Standard," Automation.com, 7 February 2009. [Online]. Available: https://www.automation.com/en-us/articles/2003-1/iec-61850-power-industry-communications-standard. [Accessed 12 October 2020].

[93] X. Huang, S. Cheng, K. Cao, P. Cong, T. Wei and S. Hu, "A Survey of Deployment Solutions and Optimization Strategies for Hybrid SDN Networks," 2018. [Online]. Available: http://www.ece.mtu.edu/faculty/shiyan/HCCCWHSurvey19.pdf. [Accessed 12 October 2020].

[94] Gartner, Inc., "Security Orchestration, Automation and Response (SOAR)," *Gartner. Inc*, 2019. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar. [Accessed 12 October 2020].

[95] R. Scalco, B. Waugaman, J. Lacoste, J. Andrews, B. Beary and R. Roley, "Integrated Cyber May 1-2, 2018," *IACD - Integrated Adaptive Cyber Defense*, 2019. [Online]. Available: https://www.iacdautomate.org/may-2018-integrated-cyber. [Accessed 1 October 2019].

[96] Statement of General Terrence J. O'Shaughnessy, U.S. Air Force, Commander, U.S. Northern Command and North American Aerospace Defense Command, before the Senate Armed Services Committee, 13 February 2020. [Online]. Available: https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-13-20.pdf. [Accessed 5 August 2020].

[97] R. Scalco, B. Waugaman, J. Lacoste, J. Andrews, B. Beary and R. Roley, "Integrated Cyber May 1-2, 2018," *IACD - Integrated Adaptive Cyber Defense*, 2019. [Online]. Available: https://www.iacdautomate.org/may-2018-integrated-cyber. [Accessed 1 October 2019].

[98] Gartner, Inc., "Security Orchestration, Automation and Response (SOAR)," *Gartner. Inc*, 2019. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar. [Accessed 12 October 2020].

[99] GlobeNewswire, Inc., "Meticulous Market Research LTC," *GlobeNewsWire, Inc.*, 10 June 2020. [Online]. Available: https://www.globenewswire.com/. [Accessed 31 August 2020].

[100] GlobeNewswire, Inc., "ReportLinker," *GlobeNewswire, Inc.*, 7 May 2020. [Online]. Available: https://www.globenewswire.com/. [Accessed 31 August 2020].

[101] A. Greenberg, *Sandworm - A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York: Doubleday, 2019.

[102] Johns Hopkins University Applied Physics Laboratory, "Johns Hopkins APL Enlists States for Cyber Defense Technology Pilot Program," *Johns Hopkins University*, 13 July 2020. [Online]. Available: https://www.jhuapl.edu/PressRelease/200713-APL-CISA-enlist-states-cyber-defense-technology-pilot. [Accessed 31 August 2020].

[103] A. Scalco and S. Simske, "Cyber-Physical System (CPS) Security Engineering Research," *Control System Security Engineering*, 2020. [Online]. Available: https://www.controlsystemengineering.info/. [Accessed 31 August 2020].

[104] T. Sherasiya, H. Upadhyay, "Intrusion Detection System for Internet of Things," IJARIIE-ISSN(0)-2395-4396, 2016.

[105] M. L Loper, B. Swenson, "Machine to Machine Trust in Smart Cities," *IEEE International Conference on Distributed Computing Systems*, 2017.

[106] E.M. Hutchins, M.J. Cloppert, R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Lockheed Martin Corporation*, 2011.

[107] Anirudh M, "Use of Honeypots for Mitigating DoS Attacks Targeted on IoT Networks," *IEEE International Conference on Computer, Communications, and Signal Processing (ICCSP)*, 2017.

[108] M. F. Razali et al., "IoT Honeypot: A Review from Researcher's Perspective," *IEEE Conference on Applications, Information and Network Security (AINS)*, 2018.

[109] Quang Duy La et al., "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," *IEEE Internet of Things Journal*, Vol 3, No. 6, December 2016.

[110] A. D. Oza et al., "Survey of Snaring Cyber Attacks on IoT Devices with Honeypots and Honeynets," *3rd International Conference for Convergence in Technology (I2CT)*, April 2018.

[111] Infosec Institute – "How To Protect Files With Canary Tokens," 2018.

[112] N. Quist, "Active Defense Through Deceptive Configuration Techniques," *SANS Institute*, 2019.

[113] X. Han et al., "Deception Techniques in Computer Security: A Research Perspective," *ACM Computing Surveys*, Vol. 51, No. 4, Article 80, July 2018.

[114] "2018 Cost of a Data Breach Study," *Ponemon Institute, IBM Security*, July 2018.

[115] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," IETF, RFC 4919, Aug 2007.

[116] D. J. Trump, *National Security Strategy of the United States of America*, Washington, D.C.: United States Government, 2017.

[117] Headquarters, Department of the Army, "Army Installations Strategy: Supporting the Army in Multiple Domains," U.S. Army, Washington, D.C., 2020.