Strategy Research Project

Exploring DoD's Cybersecurity Role for Protection of Transportation Critical Infrastructure

by

Captain David A. Crounse
United States Navy

U.S. ARMY WAR COLLEGE
Prudens Futuri
Carlisle Barracks, PA

United States Army War College
Class of 2014

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved--OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 15-04-2014	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Exploring DoD’s Cybersecurity Role for Protection of Transportation Critical Infrastructure	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Captain David A. Crounse United States Navy	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Professor William O. Waddell Center for Strategic Leadership and Development	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,617

14. ABSTRACT

In the event of conventional military attack or invasion by an adversary upon the United States, it is clearly recognized that the US Armed Forces, could legally respond swiftly and decisively to “protect and defend” the nation. However, in the instance of a cyber-attack upon a civilian target in the United States the military’s ability to respond is limited and its role is less clearly defined. The same holds true if the attack is directed against one of the sixteen sectors of US critical infrastructure (CI), such as transportation. In the case of a cyber attack conducted upon transportation CI, failing to prevent, mitigate or respond swiftly could have serious consequences for national and economic security. On the surface, DoD protection of transportation CI against cyber threats may seem to be a convenient solution to a growing problem. On the other hand, DoD involvement in the protection of privately owned infrastructure is wrought with many challenges that are borne out of the scope and nature of the cyber threat as well as the dynamics of the public-private relationship. This paper will explore the cyber threat to US transportation CI, challenges to DoD’s role and offer recommendations to improve DoD’s responsiveness.

15. SUBJECT TERMS
Public-private Partnership, Cyber War, Cyber Attack

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES** 32	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU		**19b. TELEPHONE NUMBER** *(w/ area code)*

USAWC STRATEGY RESEARCH PROJECT

Exploring DoD's Cybersecurity Role for Protection of Transportation Critical Infrastructure

by

Captain David A. Crounse
United States Navy

Professor William O. Waddell
Center for Strategic Leadership and Development
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the United States Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Exploring DoD's Cybersecurity Role for Protection of Transportation Critical Infrastructure
Report Date:	15 April 2014
Page Count:	32
Word Count:	5,617
Key Terms:	Public-private Partnership, Cyber War, Cyber Attack
Classification:	Unclassified

In the event of conventional military attack or invasion by an adversary upon the United States, it is clearly recognized that the US Armed Forces, could legally respond swiftly and decisively to "protect and defend" the nation. However, in the instance of a cyber-attack upon a civilian target in the United States the military's ability to respond is limited and its role is less clearly defined. The same holds true if the attack is directed against one of the sixteen sectors of US critical infrastructure (CI), such as transportation. In the case of a cyber attack conducted upon transportation CI, failing to prevent, mitigate or respond swiftly could have serious consequences for national and economic security. On the surface, DoD protection of transportation CI against cyber threats may seem to be a convenient solution to a growing problem. On the other hand, DoD involvement in the protection of privately owned infrastructure is wrought with many challenges that are borne out of the scope and nature of the cyber threat as well as the dynamics of the public-private relationship. This paper will explore the cyber threat to US transportation CI, challenges to DoD's role and offer recommendations to improve DoD's responsiveness.

Exploring DoD's Cybersecurity Role for Protection of Transportation Critical Infrastructure

> Our Nation is in a new era and our security is no longer protected by oceans and borders. Indeed, American achievement in the 21st Century will be intricately tied to our ability to secure our networks, primarily our critical infrastructure networks.
>
> —Representative Patrick Meehan (PA) [1]

In the event of conventional military attack or invasion by an adversary upon the United States, it is clearly recognized that the US Armed Forces, could legally respond swiftly and decisively to "protect and defend" the nation. However, in the instance of a cyber-attack upon a civilian target in the United States the military's ability to respond is limited and its role is less clearly defined. The same holds true if the attack is directed against one of the sixteen sectors of US critical infrastructure (CI), such as transportation. In the case of a cyber attack conducted upon transportation CI, failing to prevent, mitigate or respond swiftly could have serious consequences for national and economic security. On the surface, DoD protection of transportation CI against cyber threats may seem to be a convenient solution to a growing problem. On the other hand, DoD involvement in the protection of privately owned infrastructure is wrought with many challenges that are borne out of the scope and nature of the cyber threat as well as the dynamics of the public-private relationship.

The purpose of this paper is to explore the role of DoD in the protection of transportation CI. Under current policies, the Department of Homeland Security (DHS) is the lead federal agency that guides private sector cyber security of CI. First, this paper will begin with an overview of the cyber threat and the importance of the transportation industry and critical infrastructure to US national security. Next, the paper will examine the widespread use of the internet in the transportation sector and the vulnerabilities the internet presents. Then, the paper will undertake a review of strategic guidance, public-private coordination mechanisms and challenges to DoD involvement in the cyber protection of transportation CI. This paper will conclude with policy recommendations to improve transportation CI resilience in the face of the cyber threat.

The Cyber Threat

The threats in cyberspace to our nation's critical infrastructure are diverse in nature and wide in scope. The threat actors in cyberspace are governments, hacktivists, criminals and terrorists, each of whom present a distinct type of threat.[2] Most, if not all of today's cyber threats to CI fall into the categories of cyber espionage and cyber crime. To date, cyber war and cyber espionage have almost exclusively been executed by state actors. However, given the cyber realm's low cost of entry, coupled with the ongoing diffusion of cyber attack capabilities, the threat may potentially migrate towards the more destructive realms of cyber war and cyber terrorism.[3] According to the Worldwide Threat Assessment of the US Intelligence Community, " the likelihood of a destructive attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate…terrorist organizations have expressed interest in developing offensive cyber capabilities."[4] Overall, cyber attacks have been increasing. According to a report by the Financial Times, external cyber businesses experienced a doubling of attacks during the period 2012-13 over the previous year.[5] However, there is clear evidence that cyber espionage has expanded beyond the paradigm of state actor against another state actor.[6] In the fall of 2013, Chinese government hackers gained unauthorized access to the New York Times computer system.[7] Furthermore, there are increasing instances of state-sponsored espionage targeting private industry in addition to government and military networks.[8]

Cyber threats and attacks are increasing in number and intensity; however there are differing views as to the severity of the threat. In 2012, Secretary of Defense Leon Panetta compared the threat of simultaneous cyber attacks upon US CI that have the potential to be a “cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability.”[9] However, Thomas Rid offers an opposite view and states that “Cyberwar is still more hype than hazard.”[10] Likewise, Tyler Moore argues that while exaggerating the threat may be advantageous for raising the profile of an issue and creating action, there is also a downside. [11] However, Moore adds, it also has the disadvantage of giving the false impression that the situation is so dire that only a radical intervention might help.[12]

Cyber War?

There is vigorous debate over whether a cyber attack can be defined as an act of war. Consider the definition of an act of war according to Clausewitz: it has to be potentially violent, it has to be purposeful, and it has to be political. The cyber attacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria.”[13] In addition, Erik Gartzke argues against the Pearl Harbor analogy maintaining that cyber methods produce “soft kills” which are temporary in nature.[14] Gartzke states that in order to gain any advantage from a cyber surprise attack, it would have to be conducted in conjunction with kinetic actions.[15] An excellent real-world example of coordinated use of cyber and conventional attack occurred during an Israeli air attack conducted against the suspected Dayr as-Zawr Syrian nuclear facility in 2007.[16] While Secretary Panetta's remarks may sound alarmist, others recognize the significance of a parallel attack simultaneously directed at all three legs of the cyber trinity - military networks, government networks and civilian CI networks. As Amit Sharma stated, “in the current contemporary world in general and the developed countries in particular, reliance on modern technology is not treated as a luxury, but as a necessity, where all three tendencies are extensively dependent upon cyber space in one form or the other.”[17] Sharma goes on to explain that cyber warfare is capable of creating strategic effects - paralyzing a state at all levels and eliminating the will to fight.[18] However, to date, there have been no simultaneous, parallel attacks upon any nation's cyber trinity. During recent conflicts between states, such as the one between Russia and Georgia in 2007, attacks were limited to Distributed Denial of Service Attacks (DDoS) against government, media and banking websites and were not directed at critical infrastructure. Rather, these attacks were determined to be “unattributable, nonstate actor DDoS attacks” which were “not cyber war” but a criminal act of terrorism.”[19] The Georgian cyber attacks provide an example of the blurred lines between an act of war and a criminal act which add to the fog and friction of the cyber domain challenges. It also demonstrates the potential vulnerability that a DDoS could have upon transportation CI – an attack that takes no physical form yet results in the disruption or delay of essential services.

Attribution

Another aspect of the cyber realm which adds complexity to DoD involvement lies in conclusively attributing the attack to a state, non-state or individual actor. As information travels through the internet near the speed of light, an attack that may take milliseconds may not be discovered until after it is long over. Should the attack come from inside another state, there may not be enough time to communicate to the originating country in time to thwart the attack. In addition, the classification of a cyber event as a nuisance, crime or an attack may not be determined until after a thorough post-event analysis. Due to a lack of an agreed upon international standards or rules of engagement, an attack committed from within an uncooperative state upon US CI may never be positively attributed to an actor, preventing the administration of justice.

Critical Infrastructure

Critical infrastructure comprises “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.”[20] As it pertains to the transportation sector, cyber CI is comprised of air traffic control systems, surface transportation management centers, mass transit signal control systems, rail control systems and pipeline control systems.[21] As one of the cornerstone sectors of the US economy, transportation provides rapid, efficient transport of people, products and raw materials that are essential to economic prosperity. This interconnected and integrated system relies upon an infrastructure which is eighty percent owned and maintained by private industry. As will be discussed throughout this paper, the private ownership of transportation CI presents challenges for DoD participation in cyber security matters pertaining to the private transportation industry.

Transportation Industry

A properly functioning transportation sector is vital to national security and the economic well-being of the US. In addition, it’s one of the largest and most comprehensive systems in the world. Throughout the US there are over 4 million miles of road, over 138,000 miles of rail lines, 25,000 miles of navigable waterways, 2.6 million miles of oil and gas pipelines, over 5,000 public use airports and 8,000 commercial waterway and lock facilities.[22] The US transportation sector contributes more to the US than simply moving raw materials, goods and personnel. There are millions of workers employed by thousands of firms which provide the necessary services for the transportation sector. These contributions include the construction, upkeep and operation of CI and service vehicles. Overall, the transportation sector makes up 8.7 percent of US GDP.[23] The significant disruption of transportation due to a cyber attack would cause serious negative effects impacting the US economy and national security.

Sector Interdependencies

Aside from being a large part of the national and global economy, there exists "key dependencies" between sectors.[24] Of the sixteen sectors, almost all are dependent upon four sectors: Energy, Communications, Information Technology and Transportation. According to the 2010 Transportation Systems Sector-Specific Plan, "key dependencies are those that, if interrupted, could significantly impact the performance and overall resilience of the transportation system."[25] Therefore, vulnerability within the Transportation CI, if exploited, would create cascading effects throughout the other infrastructure sectors. Some examples of other sectors' critical dependencies upon transportation are: the energy sector's reliance upon transport of petroleum, natural gas and crude oil by rail, ship, barge and pipeline; the Defense Industrial Base sector's reliance upon air, maritime, rail and highway systems to transport goods necessary for the functioning of military operations; the Agriculture and Food sector's reliance upon the secure and uninterrupted transport of the food supply chain.[26] Stephen J. Lukasik provides an excellent real-world comparison of the cascading effects of a transportation sector disruption.[27] In the late summer of 2000, British protestors blockaded a number of oil refineries and fuel depots. These protests severely reduced the rate of tanker truck departures from twenty down to three departures per hour. Additionally, fuel supplies at gas stations were substantially reduced. On the morning of the seventh day since the protests began, oil companies projected that 90% of their stations would exhaust their complete fuel supply. As oil supplies dwindled, a supermarket chain began to rationing bread and milk purchases to fend off panic buying, the postal service announced possible restrictions in service, normal airline, bus and train operations were affected and a British industry group warned that due to interruption of raw materials, some production lines would be temporarily shuttered.[28] Furthermore, the disruption of the transportation sector created negative economic effects. As a result of this crisis, companies suffered a loss of over $3.5 billion and by other estimates; the fuel crisis resulted in a cost of $638 million dollars per day, or 10% of the United Kingdom's daily output.[29]

Technology's Increasing Presence in Transportation CI

Over the past two decades, the internet has become increasingly interwoven into everyday life and technology continues to play a vital role in the daily functioning of transportation CI. Furthermore, the transportation sector is becoming increasingly reliant upon Information Technology (IT) and internet connectivity. Many of these systems are categorized as industrial control systems (ICS) which include supervisory control and data acquisition systems (SCADA). Throughout the US, ICS systems are used in a variety of industries such as transportation, oil and natural gas. SCADA systems are employed as a means to monitor and control dispersed industrial assets. For example, a typical pipeline SCADA system monitors the pipeline's condition, transmitting routine information and providing alerts to a central monitoring facility, which processes and displays system information. Should a leak occur, the SCADA system alerts the monitoring facility where the problem can be evaluated and corrective measures are employed.[30] According to a report by Positive Technologies, a global Information Technology (IT) firm specializing in Industrial Control Systems, the US leads the world in the use of ICS and SCADA systems. Nearly one-third of the world's ICS systems that are connected to the internet are located in the US.[31] The US Intelligence Community's 2014 Worldwide Threat Assessment states that

> critical infrastructure, particularly the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems used in … oil and gas pipelines… and mass transit, provides an enticing target to malicious actors. Although newer architectures provide flexibility, functionality, and resilience, large segments of legacy architecture remain vulnerable to attack, which might cause significant economic or human impact.[32]

However, as connectivity increases, the vulnerability of these connected systems also increases, exposing the nation to potential debilitating attack or economic harm.

Transportation Sector Cyber Vulnerabilities

In the past, ICS and other information technology systems were exclusively designed and owned by the operating company and relied on a communications architecture located outside of the internet. Today, these systems increasingly utilize commercially available, Internet Protocol (IP) devices which are designed with efficiency and cost control taking priority over security capabilities.[33] As these systems are no longer separated from the internet, this increased connectivity now exposes these systems to the threat of tampering, sabotage or cyber-attack. Also, as wireless networking has become more prevalent in ICS, an adversary in close proximity may gain access without having any direct contact with the hardware.[34] While many SCADA users in the transportation industry have instituted protective measures, many companies remain unaware or choose to ignore the vulnerabilities. This inaction may be the result of a lack of resources, personnel, knowledge or the absence of mandatory federal technology standards designed to improve cyber security.

The transportation sector's diverse makeup of IT systems presents an equally diverse range of vulnerabilities. In the nation's maritime transportation industry, systems are used to control the coordinated movement of traffic and goods in and out of ports. The US Air Traffic Control (ATC) system is in the process of upgrading to its 'NextGen' system – a system dependent on the flow of digital information between aircraft, airline operations centers and ATC.[35] To date, there have been two separate instances in which research scientists from Canada and Romania demonstrated NextGen's vulnerability to hacking for a tiny fraction of the cost of this billion dollar system.[36] Obviously, the purity of ATC information exchange is essential for safety of aircraft operations-both on the ground and in the air. In 2003, the Sobig virus, spread through email, infected the computer system of the CSX railroad where it interfered with the ability to signal and dispatch trains.[37] In 2009, oil companies were systematically targeted for cyber intrusion, and in one instance malicious actors gained access to SCADA system data.[38] The above incidents serve to illustrate the wide ranging nature of existing and potential vulnerabilities to the transportation sector. By virtue of the scope and nature of the threat, it presents challenges which are best confronted through a collaborative team approach.

Strategic Guidance and Policy

The most recent national level strategic guidance has recognized that protecting US critical infrastructure is a strategic priority that requires the combined efforts the private sector, government and DoD. According to President Obama's 2010 National

Security Strategy, "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[39] In March of 2010, President Obama's Comprehensive National Cybersecurity Initiative (CNCI) identified cyber security as “one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter.”[40] For the DoD, this emphasis on the public-private cooperative effort represented a shift in thinking in response to the growing cyber threat. The 2008 National Defense Strategy stated that DoD played a strictly supporting role to DHS in the event of a cyber attack. Although the 2008 National Defense Strategy (NDS) recognized cyber attacks against CI posed a risk to national security and that DoD will "help respond to protect lives and national assets,” but it made no mention of cooperation with the private sector.[41] In addition, the 2008 NDS went on to add that

> in the long run the Department of Defense is neither the best source of resources and capabilities nor the appropriate authority to shoulder these tasks. The comparative advantage, and applicable authorities, for action reside elsewhere in the U.S. Government, at other levels of government, in the private sector, and with partner nations. DoD should expect and plan to play a key supporting role in an interagency effort to combat these threats, and to help develop new capacities and capabilities, while protecting its own vulnerabilities.[42]

However, DoD’s most recent guidance has appropriately shifted to reflect the direction of the 2010 NSS which emphasized a whole of government approach because “neither government nor the private sector nor individual citizens can meet this challenge alone.”[43]

DoD Strategy for Operating in Cyberspace

DoD’s 2011 Strategy for Operating in Cyberspace outlines five strategic initiatives - one of which states that “DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy."[44] According to Thomas M. Chen, the change in DoD strategy from 2008 to 2011 is due to the realization that "a broad level of cooperation with other government departments and private companies is clearly necessary."[45] This DoD initiative emphasizes increased interaction with "DHS, other interagency partners and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace."[46]

DoD/DHS Memorandum of Understanding

A renewed effort to strengthen the communication and collaboration between DoD and DHS is evident in the memorandum of agreement (MOA) regarding cybersecurity. This agreement outlines an exchange of personnel, provision of equipment and use of facilities between the entities of DHS, NSA and US Cyber Command (USCYBERCOM). The stated purpose of this MOA is "to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities."[47] Another example of the DoD-DHS partnership is the recently announced the concept of CYBERCOM National Mission Teams. The National Mission Teams will be dedicated to "support DHS and the Federal Bureau of Investigation (FBI) in defending dot-gov and dot-com domains."[48] In effect, these agreements reflect promising steps to help bridge the gap between the organizational responsibilities of DHS and DoD.

DHS's Role in Cyber Protection

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and charged it with the responsibilities to "develop a comprehensive plan for securing the key resources and critical infrastructure of the United States."[49] More specifically, the DHS is responsible for the cyber protection of US government networks (.gov domain) and is charged with guiding the public and private effort to ensure the protection and resilience of CI.[50] The Homeland Security Act also gives DHS wide ranging responsibilities related to sharing and disseminating information across the government and with the private sector. To organize and coordinate the nation's actions to protect CI and key resources, in accordance with its responsibilities of the Homeland Security Act, DHS developed the National Infrastructure Protection Plan for 2013.

National Infrastructure Protection Plan (NIPP)

The DHS produced NIPP is a comprehensive plan that guides the actions of the public-private partnership in support of national CI protection and resilience.[51] In the NIPP, each of the sixteen critical infrastructure sectors are assigned a Sector Specific Agency (SSA) which acts in a lead role to coordinate the public and private sector efforts to protect the physical and cyber aspects of CI. In addition, the NIPP provides mechanisms for coordination within and between the sectors. These mechanisms are the Government Coordination Council (GCC), Critical Infrastructure Cross-Sector Council and Federal Senior Leadership Council.[52] For the transportation sector, the DHS and Department of Transportation (DoT) share responsibilities, with DHS assuming the lead role.

PPD-21 and EO 13636

In February 2013, President Obama released Presidential Policy Directive 21 (PPD-21) and Executive Order 13636. The objective of these directives is to improve the national unity of effort towards CI physical and cyber protection. In the cyber realm, PPD-21 aims to promote "efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."[53] Furthermore, PPD-21 reemphasizes the shared responsibility of CI protection among all levels of government but also asserts that "critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient."[54] Executive Order 13636 addresses cyber CI security through improved voluntary information sharing and the establishment of a consultative process for CI stakeholders. Additionally, EO 13636 directed the National Institute of Standards and Technology (NIST) to spearhead the development of a 'Cybersecurity Framework' that will promote consensual alignment of technological and procedural standards with business practices.

In the discussion of cyber protection of CI, there is justifiably high emphasis upon information sharing between stakeholders. Since 2009 the DHS has created tools to improve the exchange of information such as the National Cybersecurity and Communications Integration Center (NCCIC), US Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Computer Emergency Response Team (ICS-CERT). The NCCIC serves the main operations center where cyber information is processed and disseminated to federal, state, local, international and private stakeholders involved in the protection of CI. In addition to sharing cyber threat information, the NCCIC provides government led incident cyber response capabilities to the private sector on an 'as requested' basis. The NCCIC also provides incident response capabilities via the US Computer Emergency Readiness Team (US CERT) and US Industrial Control System Computer Emergency Response Team (ICS CERT).

US CERT works “across multiple sectors and international borders” to fulfill its mission of “supporting prevention, protection, mitigation, response and resourcing efforts related to computer network defense.”[55] In carrying out its mission, US CERT provides incident response and defense capabilities to federal civilian agencies. Also, it provides the aforementioned services to private sector entities upon request. ICS CERT’s mission is specifically aimed at improving the security of the cyber control systems that are part of national CI. ICS CERT accomplishes its mission through incident response to the private sector and promotion of ICS related situational awareness. Together, the NCCIC and CERTs function to provide around the clock cyber information sharing and incident response to the government and private sector in support of CI protection.

One of the private sector’s information sharing mechanisms to help protect CI from physical and cyber threats is the Information Sharing and Analysis Center (ISAC) which was incepted in President Clinton’s Presidential Decision Directive 63 (PDD-63) in 1998. PDD-63’s sought to improve both the US government response and public-private cooperation against physical and cyber threats to the nation’s CI. This directive assigned lead federal agencies to coordinate government cooperation to help meet sector specific CI protection challenges. All ISACs are designed, funded and operated by the private sector CI owners and operators. ISACs serve as a “mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry” and the US government.[56] Of the fifteen ISACs, three are run by the transportation specific sub-sectors of maritime, surface transportation and public transportation. Since their beginning, ISACs have been trusted entities of private sector CI owners and operators which have improved the speed and quality of sector information sharing.[57]

Challenges to DoD Involvement

There are myriad challenges to increased DoD involvement in the cyber defense of transportation CI. In the US, the trust between the government and the people has been influenced throughout the nation's history by America's strategic culture. DoD involvement in the protection of US CI, whether it's in the transportation sector or otherwise, will require serious consideration of US strategic culture. Today the US military remains one of the most trusted institutions in the nation. In the annual survey of confidence in American institutions conducted by Gallup, the American military has ranked first every year since 1998 and has been ranked first or second every year since the surveys inception in 1975.[58] However, this does not do enough to put to rest fears that are part of American strategic culture. As Jiyul Kim stated, "American political culture evolved from a revolutionary distrust of strong central authority (kings and tyrants) and thus emphasizes the protection of individual and local rights and privileges and the principle of checks and balances over the efficient functioning of government."[59] Although this distrust is but one of the influences upon US strategic culture, its influence has pervaded America's national purpose and ideals. A recent example is the reaction of the American public to the National Security Agency (NSA) scandal involving Edward Snowden. Snowden, and NSA contractor, went public with highly classified stolen information pertaining to foreign and domestic intelligence gathering capabilities. A survey of opinion in the midst of the scandal revealed that fifty-six percent expressed concern that:

> federal courts fail to provide adequate limits on the telephone and internet data the government is collecting as part of anti-terrorism efforts. The opinion poll went on to say that seventy percent believe that the government uses the data for purposes other than investigating terrorism.[60]

However, the opinions were not all negative. Although most were supportive of government efforts to fight terrorism, the data illustrate the public's wariness of government intrusion into the private matters of citizens.

Further complicating a DoD response to a cyber event upon privately owned CI is the legal restrictions preventing the US Armed forces from participating in law enforcement operations. These restrictions are codified in the Posse Comitatus Act (18 USC § 1385) and Title 10 of US Code which stipulates that participation by a member of the US military in a "search, seizure, arrest or other similar activity" is not permitted unless explicitly authorized by law.[61] Presently, in accordance with US law, the Federal Bureau of Investigation has responsibility for leading investigations of criminal cyber activity.[62]

There are differing opinions as to how best to confront the cyber threat facing America's CI. Those arguing for increased DoD involvement point to the military's robust funding, extensive pool of expertise and the capability to conduct offensive and defensive network operations. However, aside from the trust and legal issues mentioned previously, DoD lacks the extensive relationships with the private sector and would have little to no regulatory or enforcement powers.[63] Furthermore, there would likely be extensive pushback from "civil liberties groups and Congress" in response to an increased military presence in the private sector's cyberspace.[64] Effects of militarization of cyberspace could have the unintended consequence of reducing Foreign Direct Investment in the US. For example, in the aftermath of the Snowden incident, a think tank reported that US tech companies could lose as much as $35 billion in business by 2016 as a result of reduced confidence by foreign customers unwilling or wary of data storage in the US.[65] Likewise, an increased DoD involvement in cyberspace in the may undermine the trust of key allies and global partners thus diminishing US national security and global influence.

Recommendations

The development of an international cyber rules of engagement or code of conduct would help to reduce the level of global cyber threats. An agreement, similar to United Nations Convention on the Law of the Sea (UNCLOS), would improve the ability to attribute and prosecute cyber attacks and act as a deterrent. Also, an international cyber law agreement would serve to put global pressure on countries that refuse to hold its citizens accountable for engaging in unlawful cyber activities. An example of such a code is the NATO Cooperative Cyber Defense Center of Excellence produced Tallin Manual. The Tallinn Manual is a manual on the law of cyber warfare. The manual has no legal authority, but it is an initial step in the right direction towards establishing international cyber norms. Any such agreement codifying or regulating cyber conflict and conduct would not have to enact sweeping mandates to have a positive effect. A modest agreement would begin to shape the future of international cyber law, producing a safer and more accountable international cyber domain.

At the national policy level, implementation of the baseline cyber framework put forth in Executive Order 13636. Although NIST is leading the development of this framework, it will be important to arrive at a consensual set of standards, methodologies, procedures and processes with the private sector. Private owners and operators of CI must balance the cost of security requirements with their ability to generate a profit. In the words of Tyler Moore, “many of the problems plaguing cybersecurity are economic in nature, and modest interventions that align stakeholder incentives…can significantly improve our nation’s cybersecurity posture.”[66] Incentives via the tax code may be a way to incentivize improvements in cyber security at cost level that is acceptable to the public and private sector.

A mandated requirement to disclose cyber attack information would improve the transportation CI community’s cyber domain awareness. In such a system, CI owners would be required to self-report cyber events to a national clearinghouse where the report can be de-identified and shared with the transportation community. Also, requiring disclosure of attacks would provide accurate metrics of the nature, frequency and scope of cyber attacks upon transportation CI. These metrics could then be used to improve cyber incident response procedures and technological fixes to mitigate further events.

Although DoD is not charged with the lead role in protecting CI, it can continue to build upon current relationships with the transportation sector stakeholders to more effectively respond to a cyber event. Cyber exercises provide excellent opportunities for public-private sector cooperation building and training. Depending on the level of comfort between private sector CI owners and DoD, exercises can begin at a modest level and gradually work up to a more comprehensive level as the public-private relationship matures. As a way for DoD to build trust and familiarity with the transportation sector, it could increase interaction with the three transportation ISACS. This interaction can be accomplished through an exchange of observers, inclusion of ISACS in exercises and organizing mutual training opportunities involving operational or technical topics. Should DHS and private transportation CI owners become overwhelmed with a cyber event, DoD can provide ready assistance with one of the newly formed National Mission Teams from CYBERCOM. Lastly, exploration of a cyber related partnership with the DoT may be useful in minimizing any potential seams in the transportations sector's public-private partnership. By pursuing these cooperative efforts, DoD will be capable of providing timely and effective assistance to DHS and the private transportation sector in the event of a cyber attack.

Conclusion

The cyber threat posed to transportation CI poses unique challenges to the transportation sector and to DoD. Threats from the traditional domains of land, sea and air provide a time and space buffer which allows time for threat recognition and reaction. However, the cyber domain threat negates the advantages of time and space – attacks can come without warning, can originate from every corner of the globe and be over in seconds. Complicating this matter is the size, complexity and diversity of the transportation CI environment. When compared to other government agencies, DoD may appear to be better resourced with personnel and technology to take the lead role in cyber security for transportation CI. However, legal, regulatory, resource and US strategic culture challenges must be overcome if DoD is to assume the lead role in the protection of transportation CI. DHS, occupying the 'middle ground' between the military and the private sector is better suited to remain as the lead in guiding the cyber protection of CI. The cyber threat is a complex and daunting challenge which no one entity, public or private can face alone. A collaborative, team effort from DoD, DHS, other government agencies and the private sector is the best way to successfully meet the cyber threat challenge to transportation CI.

Endnotes

[1]US Congress, House of Representatives, Committee on Homeland Security, Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, 113th Cong., 1st sess., May 16, 2013, 2.

[2] Joseph S. Nye, *Power and National Security in Cyberspace, America's Cyber Future: Security and Prosperity in the Information Age*, Vol II (Washington, DC: Center for a New American Security, June 2011_, 16.

[3] Ibid.

[4] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 29, 2014, 1-2.

[5] Caroline Binham, "Cyber Attacks on Companies Double," *Financial Times*, October 21, 2013, 20.

[6] Kevin Mandia, "State of the Hack: One Year after the APT1 Report," *RSA Conference Presentation*, 1:35-1:46, http://www.rsaconference.com/speakers/kevin-mandia (accessed March 7, 2014).

[7] Nicole Perlroth, "Hackers in China Attacked The Times for Last 4 Months," *New York Times Online*, January 30, 2013. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all (accessed March 14, 2014).

[8] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 13, 2013, 4, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed April 1, 2014).

[9] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times Online,* October 12, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0 (accessed February 22, 2014).

[10] Thomas Rid, 'Think Again: Cyberwar," *Foreign Policy* 192 (March/April 2012): 80-84, 9.

[11] Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options," in *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 4.

[12] Ibid.

[13] Rid, "Think Again: Cyberwar," 9.

[14] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*,"* *International Security* 38, no.2 (Fall 2013): 62.

[15] Ibid.

[16] Lewis Page, "Israeli Sky-Hack Switched off Syrian Radars Countrywide," *The Register*, November 22, 2007, http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/ (accessed March 19, 2014).

[17] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (February 4, 2010): 64, http://dx.doi.org/10.1080/09700160903354450 (accessed March 18, 2014).

[18] Ibid., 67.

[19] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008-2009): 60.

[20] *Patriot Act,* Section 1016 (e).

[21] According to the Department of Transportation, Transportation Critical Infrastructure is "comprised of six interconnected subsectors or modes- modes—aviation, freight rail, highway, maritime, mass transit and passenger rail, and pipelines—that transport people, food, water, medicines, fuel, and other commodities vital to the public health, safety, security, and economic well-being of our Nation." *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan,* 2010, 15.

[22] U.S. Department of Transportation, Research and Innovative Technology, Administration Bureau of Transportation Statistics, *Transportation Statistics Annual Report 2012* (Washington, DC: U.S. Department of Transportation, 2013), 1.

[23] Ibid., 50.

[24] *2010 Transportation Systems Sector-Specific Plan*, 16.

[25] Ibid.

[26] Ibid.

[27] Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack* (New York: Oxford University Press for the International Institute for Strategic Studies, 2003), 10-11.

[28] Ibid., 10.

[29] Lukasik's article uses year 2000 British Pound Values. Amount from the article have been converted to 2014 US Dollar values using the "Historical Currency Conversions," http://futureboy.us/fsp/dollar.fsp (accessed February 25, 2014).

[30] *Web O Pedia Home Page*, http://www.webopedia.com/TERM/S/SCADA.html (accessed February 22, 2014).

[31] Leb Gritsai et al., “SCADA Safety in Numbers 1.1, Positive Technologies,” http://www.ptsecurity.com/download/SCADA_analytics_english.pdf (accessed February 22, 2014).

[32] Clapper, *Worldwide Threat Assessment of the US Intelligence Community,* 2.

[33] Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security,* NIST Special Publication 800-82 (National Institute of Science and Technology, June 2011), 1.

[34] Ibid.

[35] Michael P. Huerta, *Next Gen Implementation* (Washington, DC: Federal Aviation Administration, June 2013), 40.

[36] Steve Henn, “Could the New Air Traffic Control System Be Hacked?” *All Things Considered*, August 14, 2012, 2, in ProQuest (accessed January 24, 2014).

[37] William O. Waddell et al., *Cyber Futures Workshop Report*, CSLD Study 2-12 (Carlisle Barracks, PA: U.S. Army War College, June 2012), 21.

[38] McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Attacks: Night Dragon* (Santa Clara, CA: McAfee, February 10, 2011) 7, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf (accessed February 24, 2014).

[39] Barack H. Obama, *The National Security Strategy of the United States* (Washington, DC: The White House, May 2010), 27.

[40] Barack H. Obama, *Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, March 2010), 1.

[41] Robert M. Gates, *National Defense Strategy 2008* (Washington, DC: U.S. Department of Defense), June 2008, 7.

[42] Ibid.

[43] Obama, *The National Security Strategy of the United States*, 28.

[44] Ibid., 8.

[45] Thomas M. Chen, *The Letort Papers: An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle Barracks, PA: U.S. Army War College, September 2013), 16.

[46] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyber-space* (Washington, DC: U.S. Department of Defense, July 2011), 8.

[47] U.S. Secretary of Defense Robert Gates, U.S. Secretary of Homeland Security Janet Napolitano "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," Washington, DC, January 27, 2010.

[48] Karen Parrish, "Winnefield: New DoD IT Enterprise Will Bring Transformation," *US Department of Defense/FIND,* September 12, 2013, in ProQuest (accessed April 3, 2014).

[49] 6 USC § 121(d)(5).

[50] U.S. Department of Homeland Security, "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience," March 2013, 1, https://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2012March13.pdf (accessed March 19, 2014).

[51] NIPP – available at DHS website http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

[52] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington DC: U.S. Department of Homeland Security), 11-12.

[53] Written Testimony of NPPD Executive Order 13636 and Presidential Policy Directive 21 Integrated Task Force Director Robert Kolansky for a House Committee on homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, (Targeted News Service: Washington, DC), July 18, 2013, in ProQuest, accessed March 29, 2014, 1.

[54] The White House, "Presidential Policy Directive 21," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed March 30, 2014).

[55] US Congress, House of Representatives, Committee on Homeland Security, Hearing Before the Subcommittee On Cybersecurity, Infrastructure Protection, and Security Technologies, 113th Cong., 1st sess., May 16, 2013, 9.

[56] The White House, "Presidential Decision Directive 63," May 22, 1998, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed March 30, 2014).

[57] Will Pelgrin, "The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection," January 2009, http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf (accessed March 30, 2014).

[58] Lydia Saad, "Congress Ranks Last in Confidence in Institutions," July 22, 2010, http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx (accessed September 7, 2013).

[59] Jiyul Kim, *Cultural Dimensions of Strategy and Policy* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009), 12.

[60] Carroll Doherty, “Balancing Act: National Security and Civil Liberties in Post-9/11 Era,” June 13, 2013, http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/ (accessed March 9, 2014).

[61] 10 U.S. Code § 375.

[62] 18 U.S. Code § 1030 (d) (2).

[63] Kevin P. Newmeyer, “Who Should Lead US Cybersecurity Efforts?” *Prism* 3, no. 2, 123.

[64] Ibid., 121.

[65] Sam Gustin, “NSA Spying Scandal Could Cost US Tech Giants Billions,” *Time Online*, December 10, 2013, http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/ (accessed March 14, 2014).

[66] Moore, “Introducing the Economics of Cybersecurity: Principles and Policy Options,” 4.