RedFame

International Journal of Social Science Studies
Vol. 5, No. 6; June 2017
ISSN 2324-8033 E-ISSN 2324-8041
Published by Redfame Publishing
URL: http://ijsss.redfame.com

Homeland Security in a Nutshell

Richard White[1]

[1]Ph.D., Department of Computer Science, University of Colorado, Colorado Springs, United States

Correspondence: Richard White, Ph.D., Department of Computer Science, University of Colorado, Colorado Springs, United States.

Received: March 28, 2017 Accepted: April 27, 2017 Available online: May 4, 2017

doi:10.11114/ijsss.v5i6.2398 URL: https://doi.org/10.11114/ijsss.v5i6.2398

Abstract

As the Department of Homeland Security begins its 2018 Quadrennial Homeland Security Review, it will certainly address the question "what is homeland security?". This article is meant to provide a concise overview. It begins with a definition and relates it back to the origins of homeland security. It then takes that same definition and projects it onto the DHS mission sets. It then takes a closer look at DHS missions in border and transportation security, counterterrorism, emergency management, countering weapons of mass destruction, critical infrastructure protection, and cybersecurity. It concludes with a unique argument that homeland security may be only a transient concern, and that technological change may offer a brighter future.

Keywords: homeland security, definition homeland security, border and transportation security, counterterrorism, emergency management, countering weapons of mass destruction, counter-wmd strategy, critical infrastructure protection, cybersecurity, department of homeland security, homeland security enterprise, federal bureau of investigation, quadrennial homeland security review

1. Introduction

Homeland security is about safeguarding the United States from domestic catastrophic destruction. Domestic catastrophic destruction comes in two forms: natural and manmade. For most of history, the manmade variety took the form of warfare, and required the combined resources of a nation state. All that changed with the Tokyo Subway Attacks in March 1995. It was the first deployment of a weapon of mass destruction by a non-state actor. It demonstrated the ability of small groups to wield destructive power on a scale once reserved to nation states. (Neifert, 1999) The incident presented an unprecedented new threat to national security. Designed to protect the sovereignty and interests of a nation among the community of nations, national security measures were ineffective against non-state actors. Congressional commissions chartered in the wake of the Tokyo Subway Attacks confirmed that the United States was indeed unprepared to deal with similar such incidents on US soil. The central problem was a lack of coordination between all branches and levels of government needed to thwart criminal acts with national consequences. (Gilmore Commission, 1999) (Hart-Rudman Commission, 1999) (Gilmore Commission, 2000) (HartRudman Commission, 2000) (Bremer Commission, 2000) (Hart-Rudman Commission, 2001) Subsequently, legislation was proposed to create a National Homeland Security Agency to provide this necessary coordination. That legislation was sitting in Congress when the United States was attacked on September 11th, 2001. (United States Congress, 2001)

9/11 demonstrated the ability of non-state actors to create WMD effects without the use of WMD. On September 11th, 2001, nineteen hijackers inflicted 3,000 deaths and $40 billion in damages. The investigating 9/11 Commission noted the attacks for their "surpassing disproportion". (9/11 Commission, 2004) The hijackers achieved WMD effects by subverting the nation's transportation infrastructure, turning passenger jets into guided missiles. This vulnerability had not gone unnoticed. In the wake of the Tokyo Subway attacks, which themselves had been an attack on Japanese infrastructure, President Clinton commissioned a panel to examine the vulnerability of US infrastructure. In 1997, the Presidential Commission on Critical Infrastructure Protection reported that there was no immediate threat to US infrastructure, but noted with concern the growing potential for cyber attack. Industrial control systems underpinning much of the nation's critical infrastructure were rapidly incorporating common components that were fueling the explosive growth of the Internet. The implication was that lifeline functions in water, energy, transportation, and communications would become increasingly vulnerable to cyber attack by anyone, anywhere. (President's Commission on Critical Infrastructure Protection, 1997) Acting on the commission's warning, President Clinton issued Presidential

Decision Directive #63 in May 1998 ordering the protection of critical infrastructure from both physical and virtual attack. (The White House, 1998) Without a strong central coordinating agency in place, these measures proved ineffective on 9/11.

In the wake of 9/11, the Department of Homeland Security was created by the Homeland Security Act signed into law in November 2002. In recognition of the new threat to national security from non-state actors, countering WMD, critical infrastructure protection, and cybersecurity were embedded in the DHS charter. (United States Congress, 2002) The new department which stood up in January 2003, however, was understandably focused on the manmade threat to domestic catastrophic destruction. Hurricane Katrina in August/September 2005 delivered a potent reminder of the devastating potential of natural disasters by inflicting 1,330 deaths and $96 billion in damages. (The White House, 2006) The disaster necessitated a re-orientation of the department to equally recognize the threats from both natural and manmade sources for domestic catastrophic destruction. Implicit within this recognition is the fact that you cannot stop either; just as you can't stop a hurricane, you can't stop a determined attacker. There is no absolute security. Homeland security is about risk management. Safeguarding the US from domestic catastrophic destruction entails balanced actions across the four phases of disaster: prevent, protect, respond, and recover. These actions are encapsulated within DHS mission sets. In accordance with the 2007 Implementing Recommendations of the 9/11 Commission Act, (United States Congress, 2007) these mission sets are periodically updated and published in the Quadrennial Homeland Security Review. The first QHSR was released in 2010. The most recent QHSR was completed in 2014. (United States Department of Homeland Security, 2014) The next QHSR is scheduled for 2018. The purpose for these reviews is to adjust DHS missions to align with new or emerging threats. In a larger sense the form of the threats has not changed since 2002, however, their priorities certainly have changed over the intervening years.

2. DHS Mission Sets

Border and transportation security became a priority mission for the new Department of Homeland Security in the aftermath of 9/11. This emphasis was understandable since the 9/11 attacks were perpetrated by foreign agents operating on US soil. The competing objectives of this mission are to keep hostile agents and their weapons from entering the US without impeding the flow of legitimate commerce across its borders. Accordingly, the Border Patrol, Coast Guard, Customs and Immigration, and newly created Transportation Security Administration were incorporated into the new Department of Homeland Security when it stood up in 2003. The Border Patrol maintains security along the US land border with Mexico and Canada. The Coast Guard maintains security along the US maritime border along the Atlantic, Gulf, and Pacific coasts. Customs and Immigration officials screen people and cargo for hostile agents and contraband at all ports of entry including airports. They also search for those who have overstayed their visit or are otherwise illegally residing in the country. The Transportation Security Administration oversees security for all domestic modes of transport including bus, rail, aircraft, ship, and pipeline. The basic difficulty with securing the nation's borders and transportation is the sheer scope and magnitude of the task. The United States shares over 1,933 miles of border with Mexico, and 3,987 miles of border with Canada, excluding Alaska. It has 12,383 miles of coastline that circumscribes 95,471 miles of shoreline. In 2014, 74.76 million foreigners visited the United States, and 1,016,518 legally migrated here. An estimated 11.4 million live here illegally. Traffic flow in-and-out of the country is managed at 328 official ports of entry. More than 2.1 million passengers fly over 23,750 domestic flights daily. There is no perfect screening. Against these numbers, the law of probabilities will prevail. (White, Bynum, & Supinski, 2016)

Counterterrorism also became a priority in the immediate aftermath of 9/11, and remains a top priority to this day. The 2002 Homeland Security Act made counterterrorism a core mission of the Department of Homeland Security, but surprisingly, the department has little direct authority over this task. Terrorism is defined in Title 18 Section 2331 of United States Code as a crime distinguished by motive, namely, to commit acts intended to intimidate or coerce US government. (United States Code) Individuals or groups who plot or commit crimes with the purpose of coercing US government are guilty of terrorism and are called terrorists. It doesn't matter whether the terrorists are foreign or domestic; if they break US law then they are subject to US justice. Counterterrorism, then, are activities designed to prevent or thwart terrorism. What does terrorism have to do with safeguarding the US from domestic catastrophic destruction? Certainly, terrorism may be a motive for inflicting domestic catastrophic destruction, and indeed was the motive in both the 1995 Tokyo Subway Attacks and 9/11. However, terrorism may not be the only motive that results in domestic catastrophic destruction. Why then this narrow focus? The answer is that the commissions investigating US preparedness in the wake of the 1995 Tokyo Subway Attacks used the word "terrorism" as shorthand to refer to "WMD attack by non-state actors". The unfortunate conflation of these two terms has persisted, and in many ways confuses understanding of homeland security. If indeed terrorism is the primary concern, then a Department of Homeland Security would've been created long before 9/11. Again, DHS became necessary because of the unprecedented threat to national security presented by non-state actors wielding the means to inflict domestic catastrophic destruction. It is the effect, not the motive, that is the primary concern. So, despite the terminology, the intent of "counterterrorism" is to

prevent or thwart those who seek to inflict domestic catastrophic destruction. Both the responsibility and authority for this mission reside with the Federal Bureau of Investigation. As a law enforcement agency, the FBI has legal authority to gather intelligence, conduct investigations, and arrest suspected terrorists. DHS does not have similar authorities. The FBI is a key component in the Homeland Security Enterprise consisting of both public and private agencies that perform critical roles in homeland security outside the direct authority of DHS, but with its coordination and support. With respect to counterterrorism, the DHS Office of Intelligence and Analysis provides oversight and bridges the divide between State, Local, and Federal agencies. DHS interfaces with local law enforcement and government agencies through 78 State and Local Fusion Centers across the country, and supports combined Federal efforts at the National Counterterrorism Center. In a larger sense the combined purpose of all DHS activities may be collectively termed "counterterrorism" as they relate to safeguarding the nation from manmade domestic catastrophic destruction. (White, Bynum, & Supinski, 2016)

Emergency management also became a priority after 9/11 and thrust the Federal government into a national leadership role it had not previously assumed. The disparate responses to the 9/11 attacks on the Pentagon and World Trade Center demonstrated the need to better equip the nation's First Responders, and institute better means for requesting and integrating response assets across agencies and jurisdictions. The nation's First Responders, though, supported as they are by State and Local taxes do not report to the Federal Government. FEMA, accordingly, was empowered by the Homeland Security Grant Program to elicit voluntary cooperation and develop standards across State and Local agencies. Among its first priorities was implementing a National Incident Management System predicated on the Incident Command System. The 2004 NIMS offered an organizational construct for integrating response assets across State, Local, and Federal jurisdictions, and orienting them towards common objectives identified in an Incident Action Plan promulgated by the local Incident Commander. State and Local jurisdictions were encouraged to develop Mutual Aid Agreements and help each other to the maximum extent possible before seeking Federal support. The 2004 National Response Plan stipulated the mechanisms for requesting Federal support in accordance with the 1988 Robert T. Stafford Act, and provided a compact means for delivering requested support in the form of Emergency Support Functions. The ink had barely dried on the NRP when Hurricane Katrina hit in 2005, and the ensuing confusion prompted a rewrite of the plan in the form of the 2008 National Response Framework. The NRF is predicated on a bottom-up process for requesting additional resources only when all local capability is overwhelmed or exhausted. States have significant resources at their disposal in the form of firefighters, police, paramedics, and the National Guard. A standing Emergency Management Assistance Compact allows Governors to request additional National Guard support from other States. Federal assistance can only be made available after a Governor declares a State disaster or emergency and submits a request for assistance to the President. This process is mandated by the Stafford Act and is designed to respect the sovereignty of States as stipulated in the Tenth Amendment to the Constitution. Once the President approves a Governor's request, FEMA is given responsibility for coordinating the Federal response and delivering ESF support to the States. Various Federal agencies are assigned primary and supporting roles in delivering ESF capabilities. As a support agency for all ESFs, the Department of Defense stands ready to lend Defense Support of Civil Authorities when requested. Under exceptional circumstances, the President may pre-position Federal support in advance of an expected disaster, as was the case with Hurricane Sandy in 2012. Otherwise, the Department of Homeland Security will deploy a Federal Coordinating Officer to advise the State Coordinating Officer in preparing and submitting individual Requests for Assistance. Deployed Federal assets establish a base of operations and conduct missions as assigned by the Incident Commander. State and Local officials retain control over all response and recovery operations. Of course, Federal assistance doesn't come free. In accordance with the Stafford Act, State and Local governments are committed to reimbursing the Federal government up to 25%, and possibly more of the total costs. This provision makes States understandably judicious in what Federal assistance they request. FEMA continues to elicit State and Local cooperation through the Homeland Security Grant Program. In order to guide State and Local investments towards building Core Capabilities that will decrease their dependence on Federal assistance, all HSGP participants are required to annually update a Threat and Hazard Identification and Risk Assessment. HSGP, NIMS, and NRF are generally considered successful programs, and largely credited for improving the nation's overall readiness to respond to disasters, both natural and manmade. (White, Bynum, & Supinski, 2016)

Countering weapons of mass destruction was a concern at least a decade before 9/11. After the collapse of the Soviet Union, the Department of Defense, Department of Energy, and State Department worked together to remove WMD from former Soviet republics under provisions of the 1991 Nunn-Lugar Act. Nobody wanted "loose nukes" to fall into the hands of a rogue state. Following the 1995 Tokyo Subway Attacks, that concern expanded to include non-state actors. The general strategy enunciated in later documents was 1) nonproliferation, 2) counterproliferation, and 3) consequence management. Nonproliferation included actions to prevent the further spread of WMD to those who did not have them. Counterproliferation included actions to remove or neutralize WMD in the hands of those the US did not want to have them. And consequence management entailed actions in response to a WMD attack in the US. After it was

formed, DHS joined efforts with DoD, DoE, and DoS to support this counter-WMD strategy. Within the nonproliferation arena, the DHS Domestic Nuclear Detection Office and Science and Technology Directorate seek to develop, deploy, and operate improved means for tracking WMD movement around the world. Within the counterproliferation arena, DHS border and transportation security elements are poised to intercept WMD being smuggled into the country. Of course the greater problem is that WMD agents are already here and accessible in the United States. Chemical weapons can be easily concocted from common household cleaning products. Biological agents can be nurtured from natural samples using simple techniques. Radiological sources are kept under varying levels of security in local hospitals and clinics. And there is yet no permanent disposal for spent nuclear fuel rods. For these reasons, DHS' role in coordinating Federal disaster response makes it the primary agency for consequence management following a WMD attack in the United States. (White, Bynum, & Supinski, 2016)

Critical infrastructure protection is another concern that emerged before 9/11, but is also a task over which the Department of Homeland Security has little direct authority. Direct authority for protecting critical infrastructure resides with the owners and operators of critical infrastructure assets, some of which are public, most of which are private, and some of which are regulated, and some of which are not. The framework for protecting critical infrastructure was established by PDD-63 issued by President Clinton in 1998, modified under HSPD-7 issued by President Bush in 2003, and presently maintained under PPD-21 issued by President Obama in 2013. These executive orders establish program goals and objectives, and provide the authority by which DHS now coordinates critical infrastructure protection across Federal agencies. The central coordinating mechanism is the National Infrastructure Protection Plan maintained by the DHS National Protection and Programs Directorate. The first NIPP was released in 2006. Subsequent revisions were issued in 2009 and 2013. The NIPP is comprised of two key constructs: 1) a Public/Private Partnership, and 2) the Risk Management Framework. The Public/Private Partnership is an organizational construct in which designated government Sector Specific Agencies guide the development of Sector-Specific Plans in voluntary cooperation with key industry representatives participating in various Sector Coordinating Councils. The construct is designed to facilitate a cross-flow of information and build a general understanding of the state of critical infrastructure protection within each infrastructure sector. PPD-21 identifies sixteen infrastructure sectors. This process is repeated and the corresponding Sector-Specific Plans updated approximately every four years. The first SSPs were released in 2007. The first update was issued in 2010. The most recent update was completed in 2016. The SSPs generally follow the five steps of the Risk Management Framework: 1) Set Goals and Objectives, 2) Identify Infrastructure, 3) Assess and Analyze Risks, 4) Implement Risk Management Activities, and 5) Measure Effectiveness. In conjunction with this broad management approach, DHS also works directly with infrastructure owners/operators, and State and Local governments to directly implement the steps of the Risk Management Framework. The NPPD Office of Infrastructure Protection manages the National Critical Infrastructure Prioritization Program which conducts an annual census of critical infrastructure assets in coordination with State and Local governments. DHS Protective Security Advisors conduct voluntary Site Assistance Visits and Security Surveys at the request of infrastructure owners/operators. And various FEMA grants may be employed to effect security enhancements. Unfortunately, the Risk Management Framework is fraught with problems at every step: 1) Reluctance to reveal proprietary data; 2) Multiple databases with incomplete and questionable listings; 3) No uniform analysis for comparing risks across assets and sectors; 4) No direct funding for security improvements to private industry; and 5) No established metric for guiding national strategy. As DHS has encountered difficulties trying to help industry directly, DHS has fostered the establishment of Information Sharing and Analysis Centers to help industry help itself. These have met with varying degrees of success, but have yet to realize their full potential. Meanwhile, NPPD staffs a National Infrastructure Coordinating Center to maintain watch over the nation's infrastructure and coordinate Federal support should it become necessary. (White, Bynum, & Supinski, 2016)

Cybersecurity was a recognized concern before 9/11, but only attained its current priority status with the release of the 2010 Quadrennial Homeland Security Review. The NPPD Office of Cybersecurity and Communications maintains watch over US cyber infrastructure from the National Cybersecurity and Communications Integration Center. If it spots trouble, the NCCIC can call on two cyber emergency response teams: US-CERT and ICS-CERT. If requested, the ICS-CERT can deploy teams to assist owners/operators as needed. The fact of the matter, though, is that DHS response assets are few, and their ability to contain and solve problems limited. As with all infrastructure under its protection, DHS has little direct authority over any of it. Direct authority for protecting cyber assets resides with owners/operators. The 1984 Counterfeit Access Device and Computer Fraud and Abuse Act makes it a crime to access a computer without permission from the owner/operator. A 1986 amendment made it a further crime to distribute malicious code, traffic passwords, or conduct denial of service attacks. Cyber attack, according to the National Research Council is any "deliberate action to alter, disrupt, degrade or destroy computer systems or networks or the information and or programs resident in or transiting these systems or networks." Cybersecurity is defined by DHS as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against the damage, unauthorized use or modification, or exploitation." In theory,

cybersecurity is easy. All you have to do is ensure confidentiality, integrity, and availability of a computer and its data. Confidentiality ensures that the system and data are not accessed by an unauthorized agent. Integrity ensures that the system and data are not corrupted by an unauthorized agent. Availability ensures that the system and data are always accessible when needed. These seemingly simple goals, though, are impossible to attain because computers are inherently stupid and fragile. Computers are stupid because they are incapable of making value judgments regarding their actions and will perform as directed even if the consequences are catastrophic. Computers are also fragile because with any useful piece of software you don't know what you've got and have no way of finding out. According to a 2014 study, the two primary methods of cyber attack are phishing and exploitation. Phishing is a social engineering technique designed to fraudulently obtain names and passwords from authorized users. Exploitation takes advantage of software flaws to obtain access to a computer or its data. Quite simply, there is no cure for cyber attack, nor does any present itself for the foreseeable future. The nation's infrastructure is indeed vulnerable as predicted by the 1997 presidential report. To demonstrate the point, in 2007 DHS and DoE conducted Project Aurora whereby they issued commands over the Internet causing a baseline electricity generator to self-destruct. In December 2016, a power blackout in Ukraine's capital Kiev was attributed to cyber attack. Moreover, the 2010 STUXNET attack against Iranian nuclear centrifuges proved that you don't have to be connected to the Internet to succumb to cyber attack. The potential consequences of a coordinated cyber attack against US critical infrastructure could result in the worst catastrophe in US history. Three scenarios in particular give cause for worry: 1) Undermining the US Federal Reserve; 2) Causing a meltdown at two or more nuclear power plants; and 3) Shutting down the North American electric grid. The central importance of cybersecurity today is this: cybersecurity is essential to critical infrastructure protection, which is essential to homeland security, which is about safeguarding the United States from domestic catastrophic destruction. (White, Bynum, & Supinski, 2016)

3. Conclusion

Admittedly, this view of homeland security doesn't square with most conventional understanding. Again, the unfortunate conflation of terms early on means that most equate homeland security with terrorism. Again, terrorism is incidental, not central to homeland security. Homeland security is about safeguarding the United States from domestic catastrophic destruction. The significance is not just a matter of nomenclature. By shifting emphasis from the motive to the means for committing a crime, then the problem changes from a social one to a technical one. By comparison, social problems are hard; technical problems are easy. It takes generations to change social attitudes. It takes less than a decade to change technology. As has been amply noted, both WMD and critical infrastructure provide the means for manmade domestic catastrophic destruction. Advanced tracking and detection technology can potentially contain the threat from WMD. Emerging failsafe and segmenting technologies may reduce cyber attack from a peril to a nuisance to critical infrastructure. Technology can similarly blunt the effects of natural disasters, and in many cases already has. Though it is unlikely we will ever achieve peace on earth and goodwill towards men, it is likely that technological change, both evolutionary and revolutionary, can eliminate the threat of domestic catastrophic destruction. This is a happy story because it means that homeland security may only be a transient concern. The future can be brighter. And that is homeland security in a nutshell.

References

9/11 Commission. (2004). *A Failure of Imagination: The 9/11 Commission Report*. Washington, DC: Government Printing Office.

Bremer Commission. (2000). *Report of the National Commission on Terrorism*. Washington, DC: United States Congress.

Gilmore Commission. (1999). *First Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*. Washington, DC: United States Congress.

Gilmore Commission. (2000). *Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*. Washington, DC: United States Congress.

Hart-Rudman Commission. (1999). *New World Coming: American Security in the 1st Century, Major Themes and Implications*. Washington, DC: United States Congress.

Hart-Rudman Commission. (2000). *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom*. Washington, DC: United States Congress.

Hart-Rudman Commission. (2001). *Road Map for National Security: Imperative for Change*. Washington, DC: United States Congress.

Neifert, A. (1999). *Case Study: Sarin poisoning of Subway Passengers in Tokyo, Japan, in March, 1995*. Huntsville, AL: Camber Corporation.

President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations: Protecting America's Infrastructure*. Washington, DC: The White House.

The White House. (1998). *PDD-63, Critcal Infrastructure Protection*. Washington, DC: The White House.

The White House. (2006). *The Federal Response to Hurricane Katrina: Lessons Learned*. Washington, DC: The White House.

United States Code. (n.d.). *T18 USC S2331: Terrorism*. Washington, DC: Government Printing Office.

United States Congress. (2001). *HR 1158: To Establish the National Homeland Security Agency*. Washington, DC: Government Printing Office.

United States Congress. (2002). *Homeland Security Act of 2002*. Washington, DC: United States Congress.

United States Congress. (2007). *Implementing Recommendations of the 9/11 Commission Act of 2007*. Washington, DC: Government Printing Office.

United States Department of Homeland Security. (2014). *2014 Quadrennial Homeland Security Review*. Washington, DC: United States Department of Homeland Security.

White, R., Bynum, T., & Supinski, S. (2016). *Homeland Security: Safeguarding the U.S. from Domestic Castastrophic Destruction*. Colorado Springs: Bookbaby.com.