THREAT-BASED DEFENSE

A Public Response to Emerging Exploits

Engaging Civil Defenders to Enhance the Collective Cyber Defenses of the United States

A Changed Conversation on the State of HLS Cyber Capacity

"The battle, Sir, is not to the strong alone; it is to the vigilant, the active, the brave. Besides, Sir, we have no election. If we were base enough to desire it, it is now too late to retire from the contest..."

- Patrick Henry

Introduction

This document reflects ongoing efforts to create, evolve, and refine a new community-based approach for cyber defense of the United States homeland. As part of the process of developing and evolving new cyber operational concepts and paradigms, MITRE, as the operator of DHS' Homeland Security Systems Engineering and Development Institute (HS SEDI), is engaging organizations and experts across a broad spectrum of industry, academia, and government for feedback on these evolving concepts.

A Public Response to Emerging Exploits

The scope and breadth of authorities, capabilities, responsibilities, and opportunities present in the Homeland Security (HLS) mission space are tremendous. The DHS mission includes systems, data, capabilities, and authorities that afford DHS some of the most relevant powers to defend the nation ever witnessed. The missions of intelligence, preparedness, and recovery as well as roles with the State, Local, Private Sector, and Law Enforcement communities present DHS with a treasure trove of untapped capability. However, ten years in, DHS continues to find itself partnering with traditional national security entities and struggling to find its own voice in executing the HLS mission. In each of the partnerships, DHS uses the information and capabilities of its partners and is bound by their authorities and perspectives to accomplish its unique mission. However, in each instance, the ability of DHS to contribute to the outcome of the mission can be significantly enhanced if they simply turn to their organic capabilities and change the conversation.

The intent of this paper is to highlight how DHS can reestablish its ability to execute its mission to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards"[1] and to discuss mechanisms by which to achieve this outcome. In the area of cybersecurity, DHS has been playing supporting roles or enabling its other national security partners. DHS has found itself in the position of delivering outcomes based on rules defined by legacy structures, vastly differing needs, and retrofit capabilities. Ironically, DHS has experienced this while simultaneously being granted more authority, responsibility, and money, and being appointed executive agent for the security of the .gov domain and the critical infrastructure and key resources (CIKR) elements of the .com domain.

A system failing to meet the needs of its constituents

The legacy national security apparatus is not sufficient to meet the responsibilities DHS has in its charter and the changing dynamics of the threats and hazards facing the United States (U.S.) homeland today. This apparatus is suited to serve a fraction of its constituents. The Office of the President, the Intelligence Community, and the Defense Community all have

[1]DHS, Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland, p. vii, February 2010, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

a number of channels to obtain information and exercise elements of national power. However, when it comes to the security of the homeland, DHS has not been able to leverage its organic capabilities, nor has it been able to meet these challenges using the traditional national security resources of the U.S.

The world has changed significantly since 9/11; however, the U.S. Government has remained focused primarily on enhancements to the federal posture in dealing with the threats that face the U.S. Some small measures have been implemented to varying levels of success with State, Local, and Private Sector participants, but these have fallen short of the far-reaching changes required to achieve success. Additionally, DHS has struggled to identify its constituents, to define its roles with each of those constituents, and to establish meaningful, sustainable, flexible mechanisms to engage those constituents. It has not found its voice to bring the millions of "sentinels" it has at its ready disposal – its citizens – to meet the challenges facing the HLS cyber ecosystem. DHS has not adequately informed, nor empowered, citizens to play a meaningful role in defending the nation.

THE TIME HAS COME to help unite our scattered civil defenders and their activities into a coordinated campaign more effective than anything imagined to date.

Citizens are the building blocks of the HLS enterprise. Citizens work together in businesses, in corporations, in critical sectors, in State and Local Government, in trade organizations, in Federal Departments and Agencies (D/As), and individually. Individually or collectively, citizens are the key to meeting the challenges faced by the HLS cyber ecosystem. To better involve citizens in homeland security, DHS must remove the inadvertent obstacles it has placed in its way. Citizens, in turn, must be willing to grapple with the risks they and their communities are likely to face and to embrace a more active role in preparing for the cyber challenges facing the U.S.

As the executive agent responsible for the protection of the U.S. civilian Federal D/As' networks, data, and cyber missions, DHS plays a role similar to the role the Department of Defense (DoD) plays in the protection of the .mil and .ic networks. However, DHS is not bound by the same constraints and thinking created through the hierarchical command and control-centered view that the military takes. The 2008 National Security Presidential Directive 54 (NSPD-54) and Homeland Security Presidential Directive 23 (HSPD-23), collectively known as the Comprehensive National Cybersecurity Initiative (CNCI), attempted to redefine how the U.S. thinks about cybersecurity. It called for the deployment of DoD solutions (conceived and designed for the .mil domain) to be extended to the .gov, and ultimately the .com, domains. These concepts were based on assumptions that the capabilities present in those systems could be adopted, and the threats facing the U.S. could be met, by flipping the national security apparatus around and applying it to defense. In some areas, those planning assumptions were accurate; in others they lacked rigor or were short-sighted in evaluating the viability of the threats to come and the ability to tailor solutions to meet civilian cybersecurity needs.

CNCI was the major muscle movement needed to energize the executive branch on the topic of cybersecurity and to begin the long process to improve the ability of the U.S. to address the cyber challenges. While it brought focus and money to a national problem, it fell short in application and failed to meet the needs of the constituents in the HLS portion of the equation. CNCI did not change the way the U.S. Government thinks about addressing actual cyber challenges, it did not engage the full spectrum of its constituents, and, most importantly, it did not change the way those constituents do business.

Engaging the entirety of the cyber ecosystem to address the shortcomings

An editorial article by Stephen Flynn pointed out that, in the U.S., our history of strength flows from "its citizens in times of crisis, with volunteers joining fire brigades and civilians enlisting or being drafted to fight the nation's wars. But the Cold War, keeping the threat of a nuclear holocaust at bay, required career military and intelligence professionals operating within a large, complex, and highly secretive national security establishment. The sheer size and lethality of U.S. and Soviet nuclear arsenals rendered civil defense measures largely futile. By the time the Berlin Wall came down and the Soviet Union collapsed, two generations of Americans had grown accustomed to sitting on the sidelines and the national security community had become used to operating in a world of its own."[2]

This view persists today, and is especially evident in the area of protecting the cyber ecosystem. DHS has allowed this view to smother its organic ability, preventing DHS from fostering a solution that builds upon the strength of its constituents. Cybersecurity is not solely a government problem, and the limiting factors are no longer the same as they were during the Cold War. As Flynn points out, "To an extraordinary extent, this same self-contained Cold War–era national security apparatus is what Washington is using today to confront the far different challenge presented by terrorism. U.S. federal law enforcement agencies, the border agencies, and the Transportation Security Administration are subsumed in a world of security clearances and classified documents. Prohibited from sharing information on threats and vulnerabilities with the general public, these departments' officials have become increasingly isolated from the people that they serve. This is the wrong approach to protecting the homeland. Even with the help of their state and local counterparts, these federal agencies cannot detect and intercept every act of terrorism."[3]

The threats the cyber ecosystem faces today are not limited to nation state actors with piles of sophisticated weapons and national armies trained to use them. Money is no longer a limiting factor, and technology is no longer a barrier to entry for our adversaries. The tools used to conduct legitimate business are in the hands of those who could use them for nefarious purposes. The nature of the threats present opportunities to transition from the world of traditional national security capabilities and enter a world of HLS-repurposed capabilities. These are already present and in use in the U.S. industrial complex and citizenry, and in DHS' own organic systems.

How then does the HLS enterprise meet the challenges of this world while managing expectations and being relevant to its constituents?

DHS is part of a broader HLS ecosystem. HLS is, in turn, part of a broader set of national capabilities and responsibilities. In these roles, DHS cannot afford to be the leader in providing services to every set of players. Establishing criteria by which DHS assesses its roles, actively manages those roles, and finds ways to transition new ideas and capabilities

[2]Foreign Affairs, May/June 2011, http://www.foreignaffairs.com/articles/67745/stephen-flynn/recalibrating-homeland-security
[3]Ibid.

to other members of the enterprise (and to re-engage if the threats or needs of the nation change), is the first step in maturing the DHS enterprise approach from an 'us" to a "U.S." engagement.

How does DHS turn the tide, meet the responsibilities it has in this cyber ecosystem, and ensure a homeland that is safe, secure, and resilient against terrorism and other hazards?

It does so by altering the rules of engagement.

CHANGE THE GAME: There is a unique opportunity to significantly change the game by turning to the organic capabilities of the HLS cyber ecosystem, by considering the engagement in new terms, by engaging with different equipment, and by turning to non-traditional sources of capabilities. Emerging innovations are powering a new level of capability to identify and respond to cyber threats. These innovations come not from the traditional national security apparatus but from the organizations DHS has responsibility to protect and partner with. A subset of the most advanced defenders in the HLS cyber ecosystem is seeing dramatic results from a set of advanced practices based on unclassified open source information and carefully crafted collaborative analysis across a wide range of sectors. Thoughtfully encouraged, fostered, and nurtured, the innovative collaboration combined with DHS-led defensive doctrine could be leveraged into the first piece of a true civil cyber defensive campaign.

CHANGE THE RULES: Cybersecurity is not about control, and certainly not about government control. No single organization is large enough or powerful enough to control the cyber ecosystem. To address the threats facing the U.S. today, DHS must become focused on developing partnerships with defined measures of effectiveness. There must be widespread, distributed action toward that goal, so that the approach is based on creating layered security involving partnerships, as opposed to traditional national security top-down or government-down approaches.

Successful public-private partnership (PPP) approaches that have existed for decades –have not translated effectively to the challenges of cybersecurity. First of all, cybersecurity PPPs have focused on but a subset of all possible roles - typically information sharing- at the expense of pursuing other roles, and even that subset of capabilities are often mis-executed. A majority of the current partnerships center around exchange mechanisms and models related to information (i.e., threat, vulnerability, or incident data) sharing and do not fully explore the wide range of needs of the participants who engage in partnership activities.

The successes in information sharing PPPs have occurred in those where the U.S. Government is the "big dog," and industry plays a secondary role. Limited, incredibly narrow, and singular successes have enabled discrete wins, but sustainable, broad partnerships remain more dream than reality. One size fits all, or even multiple instantiations of similar models, are not getting the job done. Instead of fighting this reality, DHS must embrace it. DHS must expand the range of potential useful outcomes of PPPs, find areas where the parties agree, and build from there. Where the parties disagree or have competing needs, DHS should not attempt to resolve all conflicts, but agree to disagree and accept that the parties may need to pursue duplicative efforts. PPPs are not only about finding ways to share, but ways to engage members of the cyber ecosystem in open dialogue, and to understand the needs, capabilities, and opportunities for future partnerships.

CHANGE THE PLAYERS: DHS' success thus far has been hampered by over-reliance on the national security apparatus. The adversary faced today is organized and persistent, and the U.S. is suffering huge losses in national intellectual property and setbacks in the ability to deliver citizen services. If the adversary is everywhere, then shouldn't the defenders be everywhere? The national security apparatus is well suited to deal with events requiring centralized command and control, but the majority of the issues and events of the cyber ecosystem are better suited to a decentralized response by its members. Engaging non-traditional HLS partners – those in industry, academia, the U.S. civilian Federal D/As, State and Local Government, and even private citizens – presents a tremendous potential for DHS to change the dynamics of the engagement.

DHS often finds itself attempting to be all things to all parties, and as a result has overcommitted and often under-delivered. To improve in this area, DHS must define its role(s), stay focused on only those roles, and enable other members of the cyber ecosystem to perform their roles. Innovation and adaptability are not strengths of the U.S. Government. However, the ability to absorb costs, remove legal obstacles, and sustain capabilities in the face of crisis are attributes which should be fostered and benefited from. Moving opportunities forward requires DHS to examine its partnership roles, requirements, and responsibilities, and to proactively seek out, carefully craft, nurture, and strategically execute multi-faceted partnerships. DHS must be many things to many parties, and not employ one-size-fits-all approaches in engaging with its partners and constituents. The span of its constituents, missions, and capabilities dictate that DHS may sometimes act as trusted leader, in certain cases as a funder, and frequently as a catalyst, facilitator, and participant.

CHANGE THE EQUIPMENT: Consider the well-known metaphor of the needle and the haystack. There are two ways to hide a needle: the first is in that haystack and the second is in a stack of needles. The same tools cannot be used to find the needle in both stacks. So what can DHS do to ensure they are able to apply the best tools to solve the problems facing the American people?

For too long, DHS has been working with the leftovers from legacy national security precepts and programs. It has been required to use systems, approaches, and technology from its national security partners, and not allowed full authority to define its unique requirements and use its differences as strengths to find solutions to these challenges.

Advanced analytic tools, data aggregation, authentication technologies, and even the sensors DHS uses to collect cyber events can be provided via alternative sources. Government off-the-shelf (GOTS) or even Defense Industrial Base (DIB)-style commercial off-the-shelf (COTS) solutions are limited in what they provide. Recent approaches used by select companies to alert users to threats indicate that some members of the cyber ecosystem are using technical solutions that are neither conceived nor funded by the U.S. government to meet the challenges they face. Utilizing health care, finance, marketing, or music industry approaches to collecting, integrating, sharing, protecting, or leveraging cyber information will provide DHS with organic capabilities that complement the traditional national security cyber situational awareness capabilities. As a by-product of engaging its constituents in these changed approaches, the technology leveraged may lead to business models, lines of business, or technical capabilities which can be offered back to less sophisticated constituents.

Engaging civil defenses to enhance the collective cyber defenses of the U.S.

This simple concept has too long been relegated to speeches and platitudes. DHS has a defensive mission. It can choose to be defensive in its approaches or it can be proactive in charting its defensive approach. Today, isolated defenders sit in their foxholes in a reactive posture waiting for the next attack, defending against proximate attacks and responding at the local level. The small subset of defenders that have banded together, sharing tools, techniques, warnings, and experiences, have significantly improved results. The national interests demand that this style of innovative collaboration be made accessible to the entire civil sector.

Standing at the gates to some of the hardest challenges this nation faces, both technically and conceptually, DHS can realize the vision of creating a safe, secure, and resilient cyber environment that enables and fosters innovation and prosperity for the entire nation. This vision should serve as a guide post, not a hitching post. To deliver against that vision, the U.S. needs a variety of teams to drive and sustain a safe, secure, and resilient cyber infrastructure through innovative leadership, expertise, and strong strategic partnerships in support of the HLS mission. The entities to help us meet the challenges come not from some secret fort, or some remote operating location, but from the very resources organic in the HLS ecosystem- cyber and otherwise.

The time is now. The need is growing. Vanguard elements are working these ideas and finding others with like minds, one by one. Many are weary of losing the battle, and would do more if educated and invited. As with the American Revolution, let us respond to the brute force of our attackers collectively and adaptively, and change the game by altering the rules of engagement.

Acknowledgments

This paper was written by The MITRE Corporation, in collaboration with and funding from the Deputy Assistant Secretary of Homeland Security, Cybersecurity & Communications (CS&C), through the Department of Homeland Security FFRDC (Homeland Security Systems Engineering and Development Institute (HS SEDI)) under contract # HSHQDC-09-D-00001

MITRE