CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Cyber Policy Task Force

Working Group Discussion Papers

The Discussion Papers

The following papers were used to generate discussion and debate within the Task Force. The views expressed in the discussion papers are the views of the authors of each respective paper.

Table of Contents

Fixing The Department of Homeland Security

Daniel Chenok

Karen Evans

Robert Lentz

Bobbie Stempfly

Introduction

The US is no longer on the cutting edge in organizing for cybersecurity. Other nations are experimenting with models that are different, and, perhaps better, than what the US adopted in 2009. To be fair, the US is larger than most of these countries, with thousands of critical infrastructure companies and gigantic agencies. While the creation of a Cyber Coordinator in the National Security Council (NSC) did much to reduce Federal disorganization, there are still problems.

The biggest problem is DHS. While the current leaders of DHS have significantly transformed the agency, crucial flaws remain. CSIS's 2009 report recommended the creation of a stand-alone cybersecurity agency (the model most other nations have now adopted), but this administration chose in 2009 to make DHS the focal point for the national cybersecurity effort.

There were two problems with this. The administration did not define the cybersecurity mission other than in lofty, non-implementable terms and DHS did not have the capabilities it needed. The last few years have seen significant improvement, but to turn DHS into the real cybersecurity center, the next President must define the DHS mission, make cybersecurity an independent, operational component, and prove adequate resources for the agency.

Defining the DHS Mission

We can start by saying what DHS National Protection and Programs Directorate (NPPD) is not – it is not a law enforcement or intelligence agency. DHS's job should be to deal with the attack, not the attackers. This focused mission has three parts. First, DHS must be able, supported by NSA, to mitigate major attacks, particularly on critical infrastructure. This means having personnel who can respond, repair and restore the networks that fall victim to cyber-attack. This mission does not include retaliation or punishment. DHS cannot be a national fire department, responding to every incident: there are too many. But it cannot be a bystander. DHS needs deployable teams who can restore critical services and prevent collapse in critical sectors.

Second, DHS, working with NSC, OMB, and GSA, must master its role of defending civilian agency networks in the Federal government, extending its success with CDM (Continuous Diagnostics and Monitoring). Finally, DHS must build on its recent successes and become the hub of information sharing, not controlling but ensuring coordination and equity among firms and sectors. A focused mission statement would read:

> *The Department of Homeland Security's National Cybersecurity Agency will lead the national cyber defense to protect critical infrastructure and federal agencies, to mitigate the effect of cyber-attacks, and to ensure public awareness of serious cyber threats.*

Making cybersecurity an independent, operational component

Cybersecurity was an afterthought when DHS was created. The best evidence of this is that cybersecurity was made a headquarters support element rather than an operational component agency like Coast Guard or Customs and Border Patrol. Times have changed, but cybersecurity is still a part of the Secretary's Office. It should be separated and made independent. We suggest the name "National Cybersecurity Agency."

A flawed assessment of risk lies behind the creation of NPPD. After 9/11, political leaders were concerned that terrorists would launch attacks on physical infrastructure. This has proven to be an invisible risk in the last fifteen years. In contrast, hostile probes of critical infrastructure networks by foreign opponents are routine, with a demonstrated capability to cause disruption and destruction. DHS needs an agency that is focused on the cybersecurity problem.

Focusing on cybersecurity means shedding some peripheral functions. NPPD manages the Federal Protective Service (FPS), the agency that provides guards for Federal buildings. DHS has argued that FPS can play an important role in cybersecurity. We did not find this persuasive and FPS should be moved to another part of the agency.

Provide adequate resources. Cybersecurity is an important part of the DHS mission, but is poorly resourced compared to other parts of the agency. A serious effort would increase both funding and workforce once the DHS cybersecurity mission is clearly defined.

NPPD Reorganization Proposal – CSIS Ad Hoc Evaluation Group

Daniel Chenok

Karen Evans

Bobbie Stempfly

Introduction

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) are proposing the reorganization as outlined in the supporting attached documentation. This "transformation" as described by NPPD attempts to achieve three key priorities:

- Greater unity of effort across the organization;
- Enhanced operational activity; and
- Excellence in acquisition program management and other mission support functions.

Chairman McCaul's staff requested we review the proposal and provide insight and recommendations. The group considered the following factors as they relate to the overall assessment of the DHS reorganization proposal:

- Will it position DHS to better fulfill its mission?
- Would the separation of operations from the partnerships create unnecessary stovepipes?
- Should there be a new leadership structure with this realignment?
- What are pros/cons of integrating cyber and physical infrastructure protection elements of DHS? Will this dilute the cyber mission?

Summary of Conclusions

- The most important part of the reorganization is that the 'new NPPD' must operate like a component of Transportation Security Administration (TSA), Customs and Border Patrol (CBP), Federal Emergency Management Agency (FEMA), rather than be an element of the Office of the Secretary of DHS. This could require legislative approval if reorganization is to be meaningful.
- The Office of Biometric Identity Management (OBIM) needs to be moved out of NPPD to CBP.
- A majority believed that the Federal Protective Service (FPS) needs to be moved out of NPPD to improve operational focus, but others felt this would unhelpfully diminish NPPD.
- NPPD needs a new name.
- The "cyber-physical" alignment was the most contentious issue in our discussion and we did not reach consensus. We defer to DHS on this, noting that there are arguments both for and against it, e.g. potential benefits from combing the two versus the potential risk of distracting DHS from the cyber mission.
- Similarly, while there are arguments both for and against keeping emergency communications as part of the new NPPD, we defer to DHS on whether to keep it as part of the new organization.
- Moving the new NPPD out of the Office of the Secretary is essential to improve acquisition processes. If it does not, this may require legislative solutions that give NPPD greater flexibility and agility in acquisitions authorities.
- This plan comes relatively late in the administration. DHS has had program implementation problems the past. If DHS cannot put the reorganization in motion before March 2016, it should be postponed for the next Administration.

Below, a summary of discussion points is provided for each of the items proposed by DHS's NPPD. There was general agreement that each proposed change should require an articulation of how it ultimately improves the organization's ability to execute its mission, including a justification and transition plan to minimize disruption to the present mission and workforce.

Change the name of NPPD to Cyber and Infrastructure Protection

This name change should be based on the final decision(s) of what functions remain with the new organization.

Realign operational activities to three directorates

The chief concern is that this integration of physical and cyber will unavoidably dilute the focus on the cybersecurity mission. NPPD currently includes various functions (cyber, IP, FPS, and OBIM). While the current organization houses these functions, the structure does not integrate them effectively. Those who support the reorganization argue that DHS will be most effective in its critical infrastructure and risk management missions by having one structural organization for cross-sector coordination, encouraging adoption of the NIST framework through the C3 Voluntary Program, etc. Part of the group believes the proposed move of some of the partnership functions from cyber to IP would enhance this effort (see more below).

Work to improve Industrial Control Systems security is the most important justification of the intersection between cyber/physical. The proposed reorganization strikes the best balance between combing the operational capabilities of ICS-CERT, US-CERT and the NCCIC.

Recognizing that we currently have an organization that houses both cyber and IP, it is less disruptive in the near term and ultimately more effective in the long term to improve integration. Those in the group who support the proposed reorganization recognize that it has affected the current organization (particularly in the cyber partnerships office), and there will continue to be harm to the workforce (and perhaps the mission) as reorganization moves forward, but they note that DHS believes it can minimize these affects as it moves forward.

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC should be the center of the organization. The operational functions should include the National Communications Center (NCC) with National Infrastructure Coordinating Center (NICC) on the same Watch Floor. We recognize that an alternative would be to give FEMA responsibility for emergency communications with their disaster function. The Operations Coordination and Watch Center should be integrated into the NCCIC.

Some in the group believed that "operational" means having the mass, capabilities, and purpose to engage in all aspects of cybersecurity. This includes situational awareness, incident response, private sector engagement, acquisition, etc. While the NCCIC is the "hub" of operations - it is not in and of itself the sole operational capability this new DHS organization should bring to the mission.

Infrastructure Protection

This was the most contentious issue in our discussion of reorganization. While we would defer to DHS on the merger, we note that the premise behind the reorganization is questionable, as only cybersecurity threats to critical infrastructure are increasing, not physical attacks. Terrorists have

not focused on attacking critical infrastructure.

Private sector practice in this area is mixed, with some companies separating cyber and physical responsibilities while others combine them. The most common division in corporations is to have a single security group (under the CSO), and divide this into two subgroups, with one responsible for cybersecurity and another for physical security, with both reporting to the same leadership.

An alternative approach would be to move this mission to FEMA, since both the missions and the regional divisions of FEMA and NPPD IP activities are similar. Given the FEMA regions have well-built supporting infrastructure, some believed that it could make sense to move this directorate to FEMA. By doing this, it would also support the current industry trend of having physical and cybersecurity separated. Others believed that FEMA's emphasis on response would weaken the infrastructure protection mission.

DHS's role in Infrastructure Protection is as important, but it does not need to be part and parcel of a single operational organization or directly tied to the cybersecurity organization. What is necessary is that the physical mission – again operationally – is aligned and capable of functioning in real time with the operational cybersecurity organization. Both do not need to be led by a newly named NPPD organization. It may also be a mistake to separate cyber policy from the operations and technology, as they are interdependent.

Federal Protection Service's law enforcement and security operations

The fundamental difference among group members is that many believe that FPS dilutes the cybersecurity mission, while others believe it can be integrated into cyber security in helpful ways, noting that if electrical or ICS systems in buildings fail, it is not clear immediately if this is the consequence of a cyber action or something else.

Most of the group agreed this function should move out of NPPD. The primary mission of FPS is neither cybersecurity nor infrastructure protection. However, there was a difference of opinion of where it should move. Several members were in favor of moving this function to the US Secret Service while others recommended moving the function back to the General Services Administration (GSA) as FPS is part of the building services provided by GSA. Some also feared that sending FPS to Secret Service at such a complicated time in the Service's history would be difficult operationally and politically.

The group agreed that the Office of Biometric Identity Management (OBIM) should be moved to CBP.

Establish an Acquisition Program Management function

The functions included in this proposed directorate such as program management, strategy, policy and planning would be needed if and when the NPPD is moved out of the Office of the Secretary and "re-established" as an operational component of DHS, similar to other operational components. This is an essential step.

DHS proposes a dedicated acquisition directorate support function, with a director overseeing staff embedded in the various programs. Frankly, this model already works with their OGC staffing and should be implemented immediately. The new directorate must be empowered with

decision-making authority of the Chief Acquisition Executive for Cyber/IP decisions. Interviews with service providers and others suggest that the pace and complexity of the acquisition has been a problem for DHS programs and finding ways to streamline and accelerate it is crucial for better performance.

Finally, answers to the questions posed regarding the overall assessment of the DHS reorganization proposal is provided below.

Will it position DHS to better fulfill its mission?

Given the discussion of the group, the current proposal as submitted by the NPPD has "some" merit if it focuses NPPD on the cyber mission and makes it an operational component. The most important change is to take NPPD out of the Secretary's office and make it an operational component.

Some in the group believed that what should drive any reorganization would be for DHS to increase its capability, competency and credibility in its national cybersecurity mission, focus on clearly articulating that mission, and create an "operational" organization that can carry out that mission. Too much time and effort is spent trying to justify the need for collocating physical and cyber vice ensuring capability exists for both and that processes and procedures are put in place for both to work seamlessly together. Collocation does not equate to greater capability. Trying to reorganize NPPD as proposed diminishes current capabilities and will neither be effective or efficient.

Would the separation of operations from the partnerships create unnecessary stovepipes?

A primary area of concern about the current reorganization has stemmed from confusion about how the plan will affect the current CS&C partnership personnel, and whether moving this function from the NCCIC will cause confusion for critical infrastructure partners and reduce the effectiveness of the DHS partnership staff. The plan DHS has articulated would keep the tactical and operational relationships within the NCCIC, while moving policy and risk management functions integrated into IP. DHS could provide value to their partners by focusing on operations.

Should there be a new leadership structure with this realignment?

We believe it is essential to make NPPD an operational component of DHS. This is necessary for improved performance.

What are the pros/cons of integrating cyber and physical infrastructure protection elements of DHS? Will this dilute the cyber mission?

The group's discussion centered on the experience in both government agencies and in the private sector in attempting to merge physical and cyber security. In actual practice, it does not appear that the alignment of Safety and Compliance Officers who traditionally handle "guns, gates and guards" with the Chief Information Security Officers (CISOs) is the norm. The private sector trend is to integrate traditional information technology (IT, CIO) and IT security functions, not cyber and physical.

A key challenge for DHS is mission focus; this is why we have recommended moving extraneous functions from NPPD. The proposed reorganization makes cybersecurity a

component of a larger mission of infrastructure security rather than the sole focus, a move that could dilute the cyber mission if DHS is not careful.

Additional Considerations/Recommendations

There were two additional recommendations made by members of the group which are not necessarily addressed or included in the NPPD realignment proposal. Both of them are related to cybersecurity workforce issues. They are as follows:

- The operation function NPPD is now performing to support the cybersecurity workforce currently resides with the Office of Cybersecurity and Communications (See https://niccs.us-cert.gov/home/about-niccs.) Although there is no statutory authority for DHS to perform this function, it is attempting to lead a national effort to support cyber education, using the National Initiative for Cybersecurity Education (NICE). NICE is led by NIST, which does have the statutory authority.

  Given the need for an overall strategy for cybersecurity workforce issues for both public and private sector, the group recommends the establishment of a new DHS office similar to the DHS Office of Health Affairs, to be called the Office of Cybersecurity Workforce. This new office would provide the overall strategy to address the cybersecurity workforce issues. Some of the authorities currently residing with NIST for NICE should be transferred to this new DHS entity. However, all the operational aspects of this program should be transferred out of NPPD to more appropriate organizations such as NIST, DoD, NSF or OPM.

- Building upon the "NET Guard" authorized in P.L. 107-296, Section 224, DHS leadership / the new Administration should consider creating a National NET Guard for cyber response capabilities, which at minimum would include a method for identifying recognized experts. This National NET Guard would allow identification of existing capabilities both within the government and within private sector; establish and maintain national experts who can assist during a cyber incident in support of disaster responses at national regional, state, and local incidents as the first 24 hours are critical. A National NET Guard would answer the need for the "first responder capability" to protect the nation in event of a large-scale cyber-attack.

The Role of Shared Services and the Cloud in Enhancing Cybersecurity

Daniel Chenok

Karen Evans

Bobbie Stempfly

Introduction

Most federal agencies are not in the security business. As incidents like the massive data breach at the Office of Personnel Management continue to remind us, protecting cyber assets is not a core competency of most agencies, nor should it be. While much is being done to increase the number and skill level of cybersecurity staff, expecting every organization to be cyber-competent is unrealistic. Federal agencies do not build cars or telephone switching systems, although most are heavily reliant on them to perform their day-to-day operations. Why do they continue to build and operate information technology systems?

While the current Administration prioritized the move to shared service and use of the cloud, these efforts need to be accelerated. Initiatives like the General Services Administration's (GSA's) FedRAMP program are developing the tools for agencies to assess the cyber-competence of cloud service providers. Apart from efficiencies, which can be substantial, shared services and the cloud allow the concentration of scarce cyber resources.

This is not an ideological argument for private sector v. public sector competence or efficiency. Rather, it argues for a return to a principle first articulated in Peters and Waterman's seminal work, "In Search of Excellence." Simply stated, effective organizations "stick to their knitting;" they do what they are best at and rely on others to provide everything else.

Recommendations

The next Administration has a unique opportunity to move beyond aspirational goals to a new reality. We propose a simple multi-step program:

1. No further investments should be permitted in agency-specific business support systems; e.g., personnel, payroll, accounting and finance;
2. Agencies currently operating such systems must provide a timetable for migration of those services to shared service provider;
3. Commission an independent evaluation of shared services currently being provided by program agencies; e.g., The Department of Agriculture or the Interior should continue to be located there or under a separate agency;
4. Identify specific program areas that on their surface appear to be agency-unique, such as medical care information management and develop specific timetables for each for the development of common infrastructure to support them; and
5. Require agencies commission independent assessments for services that are demonstrably unique due to their nature or scale of the feasibility of turning to third party service provider to operate and protect the infrastructure on which they reside.

If Google, Amazon, Microsoft and other Cloud entities where reliability is a major business risk, are already building out highly resilient networks and infrastructure, why, for example, did the Social Security Administration need to build another service center?

As part of this multi-step program, the shared services should:

1. Focus on cybersecurity as a priority;

2. Integrate to produce a "roadmap" approach to integrate cross-agency performance (CAP) goals for cybersecurity with all shared services initiatives; and
3. Expand the existing Information Systems Security Line of Business (LoB) to include security operations centers (SOC) and network operating centers (NOC) and other security service offerings to address common solutions and services.

Critical features of the shared service model:

1. Federal shared service providers need to maintain competitive pricing with private sector providers;

2. Providers, regardless of federal or private, should maintain all necessary security settings and be subject to red team/blue team testing;

3. Providers are subject to security and performance metrics and if they do not meet their performance metrics, they will be responsible for federal agencies' migration costs to a provider who can provide the service at the established metrics;

4. OMB will restrict new starts in all shared services areas, to ensure that security is a key element of any new start; and

5. General Services Administration (GSA) cost recovery model will change to avoid the service charges to agencies.

What are shared services? What has been done?

Shared Services is one of the 8 management-focused Cross-Agency Priority goals[1]:

> *The Federal Government will leverage the Executive Councils to develop common standards and benchmarks to measure shared service utilization, performance, and cost. Mandate those standards and benchmarks for common administrative services. From these standards and benchmarks, we will drive efficiencies and greater performance by: 1) increasing the capacity of the Federal Shared Service Providers (SSPs) at DOI, USDA, Treasury, HHS, DOT and DoD, and 2) requiring the use of lower-cost, higher-performing Shared Services for all agencies and SSPs which cannot meet established targets. We will target the following areas for Shared Services (listed in order of priority) financial, HR, technology, and acquisition.*

The Shared Services goal has four pillars:

1. Governance: launched the Customer Council, which includes the CFO Act agencies and the Small Agency council, and continued the Provider Council;

[1] Cross-Agency priority (CAP) goals are a tool by executive branch leadership to accelerate progress on Administration priority areas and requires collaboration between multiple agencies. The cross-agency priority goal setting was established as part of the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act of 2010). Currently, there are 7 mission-oriented and 8 management-focused goals established. (See http://www.performance.gov.)

2. Policy: issued OMB M-16-11, Improving Administrative Functions Through Shared Service with a Franchise Fund Working Group, to analyze current funding authorities to better support shared services;

3. Demand Management: developed and released the first draft of the Modernization and Migration Management (M3) Framework; and

4. Supply Management: launched the collection of service offerings, cost and quality metrics for shared service providers known as *ProviderStat*.

Additionally, the Federal Chief Information Officer (CIO) Council released the Federal Shared Service Implementation Guide dated April 16, 2013 in support of the Federal Information Technology Shared Service Strategy dated May 2, 2012 released by the White House.

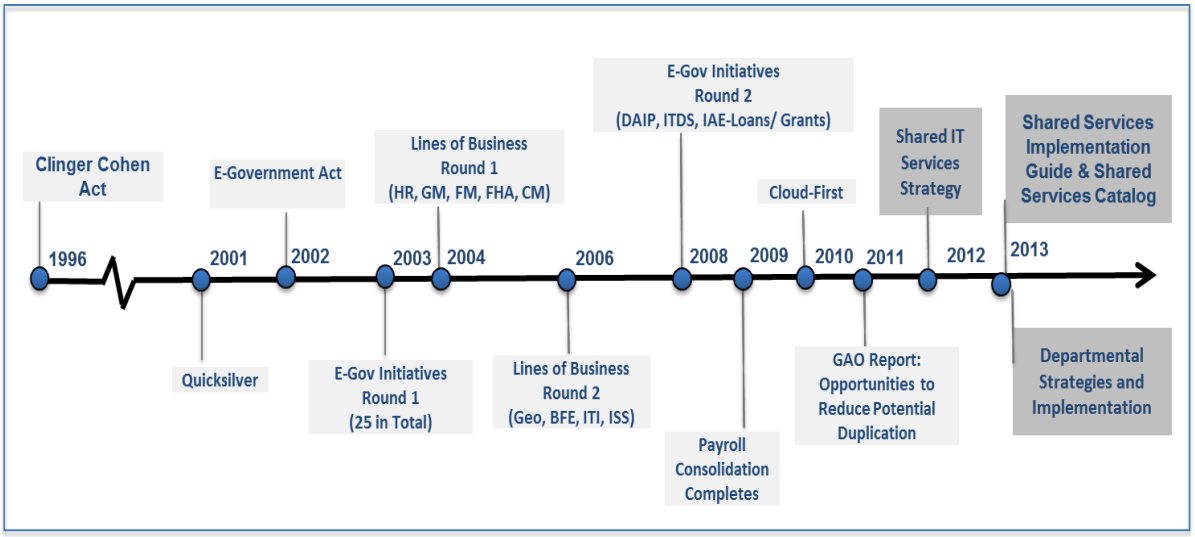


Figure 1: Timeline of Shared Services Initiatives in the US Federal Government

To support the movement to shared services, another initiative, Data Center Optimization Initiative (DCOI), OMB-M-16-19, dated August 1, 2016, states:

> *…to promote the use of green IT by reducing the overall energy and real estate footprint of government data centers; reduce the cost of data center hardware, software, and operations; increase the overall IT security posture of the Federal Government; and shift IT investments to more efficient computing platforms and technologies.*

This initiative designates the General Services Administration (GSA) as the managing partner with the Unified Shared Services Management Office share to establish and maintain a data center services marketplace. The target metrics include:

1. Optimization: energy metering; power usage; virtualization; server utilization and automated monitoring; and facility utilization;
2. Cost Savings and Avoidance; and
3. Closed Data Centers.

The Shared Services initiative is focused on the administrative back end services but there are additional lines of business (LoB) and shared service providers including:

1. Budget Formulation/Execution
2. Federal Health Architecture (FHA)
3. Financial/Grants Management (FM/GM)
4. Geospatial (GIS)
5. Human Resources (HR)
6. Information Systems Security (ISS)

**See Table 4: Federal Lines of Business in Appendix II of the Federal Shared Services Implementation Guide dated April 16, 2013.*

When analyzing the overall IT portfolio, the following questions remain unanswered:

- Why does the federal government own the information technology?
- With the Federal Shared Services providers, why are agencies providing these services when they are available commercially through cloud providers, software as service providers, etc.?
- Why aren't the shared services integrated and focused on improving cybersecurity?
- Why do program agencies provide shared services at all; specifically:
  - How does the running the National Finance Center within USDA align with the mission statement, provides "leadership on food, agriculture, natural resources, rural development, nutrition, and related issues based on public policy, the best available science, and effective management."[2]
  - How does running the National Business Center within Department of Interior align with the mission statement, "protects and manages the Nation's natural resources and cultural heritage; provides scientific and other information about these resources; and honors its trust responsibilities or special commitments to American Indians, Alaska Natives and affiliated island communities?"[3]

Discussion

While the foundation has been laid and some progress has been made to address the risk associated with agency services, the push toward shared services should at minimum be continued but with the ultimate goal of having agencies are only managing services and not buying software and infrastructure except where such infrastructure required to perform an agencies' mission is unique. An enterprise view should be taken in order to provide a "roadmap" approach which would integrate the CAP goals for cybersecurity with the Shared Services initiative focused on administrative services, DCOI, "share first," "cloud first," and other LoBs such as the Information Systems Security in order to reduce the risk of the federal government agencies and their own management/development activities.

Organizations such as the Shared Services Leadership Coalition believe you need legislation to make shared services a reality.[4] However, there is much that can be completed under the

[2] See http://www.usda.gov
[3] See http://www.doi/whoweare/Mission-Statement.
[4] See http://sharedservicesnow.org/

existing authorities included in the Clinger-Cohen Act, E-Gov Act and FITARA to consolidate and eliminate IT infrastructure thus reducing the attack surface for the federal government as whole.

At a minimum, the Information Systems Security LoB should be expanded to include the implementation of common solutions for security operations centers (SOC), network operating centers (NOC) and other security service offerings. Taking a tiered approach to capabilities and building upon the work of the General Services Administration (GSA) for FedRAMP and applying to the Shared Services model for security solutions would assist agencies with the implementation of newer technologies and also reduce risk. Additionally, the tiered capabilities would need to be "continuously tested by DHS in operations mode" to ensure the shared service providers are maintaining the security settings necessary. If the shared service providers do not meet these continuous testing/monitoring, then DHS would have the ability to "disconnect" the shared service provider until the issue(s) have been addressed.

Critical features of the shared service model include:

- Federal shared service providers need to maintain competitive pricing with private sector providers;
- Providers, regardless of federal or private, should maintain all necessary security settings and be subject to red team/blue team testing;
- Providers are subject to performance metrics and if they do not meet their performance metrics, they will responsible to costs of federal agencies migration costs to a provider who can provide the service at the established metrics; and
- OMB will restrict new starts in this area similar to DCOI initiative.

The Administration may also want to consider changing the GSA cost models in order to remove the "service charge" which GSA has to charge agencies since they are cost recovery. Agencies believe they are saving funding because if they do it themselves they are not paying the service charge. However, the agency doesn't take into consideration their true costs of managing the life cycle of the investment.

A Time for Change: The Cybersecurity Workforce

Introduction

The state of cybersecurity continues to resemble, the world of medicine and public health at the turn of the 20th century. We see growing threats in an increasingly interconnected world and a workforce of practitioners, some knowledgeable and highly skilled and other less so. The challenge is exacerbated by three factors:

1. A serious shortage in the number of skilled professionals, variously estimated to be 14,800 in the U.S. alone;[5]
2. A fundamental change in the required competencies to defend systems over the fool's errand of trying to prevent cyber intrusions; and
3. The absence of a system of validated indicators – e.g., accreditation of institutions of learning and individual professional certification – that can inform consumer choices. The consumers in this instance are both those who buy cybersecurity services or employ cybersecurity talent as well as individuals contemplating entering the career field.[6]

Yet another complicating factor is the dynamic nature of the problem. As the technology grows more complex and threats, intended or not, grow more sophisticated, we need professionals who keep current and a career field in which subspecialties that we may not have anticipated becoming critical to protecting our cyber infrastructure.

It has been eight years since the identification of the cybersecurity workforce crisis by the Center for Strategic and International Studies, as authors drew attention to this foundational challenge: "The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government."[7] The situation has only grown more precarious as efforts to better define roles and competencies have failed to lead to any game-changing results. The rapid growth in demand fueled by greater automation and robotics is driving a greater divide between needs and available workforce. The growing demand requires newer competencies and skills, which only further stretch the available workforce. And as we face significant and ever-changing new challenges, progress in addressing past threats for which remedies are well-known is at best uneven. Eight years ago the world was introduced to the Conficker Worm, a technical threat that took advantage of a Microsoft vulnerability to self-propagate and invade networks. The remediation of this threat has been available for 8 years and this threat continues to infect systems all around the world.

[5] According to the Bureau of Labor Statistics' Occupational Outlook Handbook (see http://bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6),

[6] The work of this taskforce was focused on those who perform cybersecurity functions. Users of technology play an important role in "staying safe" and user awareness programs are important but our systems must be built to be able to withstand the misdeeds of those who seek to do harm and the neglectful actions of uninformed users.

[7] Center for Strategic and International Studies, Report of the Commission on Cybersecurity for the 44th Presidency, December 2008

Our Vision

It is eminently possible by 2020, the end of the next President's first term, to have developed and fully implemented an education and workforce model for cybersecurity with the following attributes:

- A system for accrediting training and educational institutions that offers programs in either theoretical or applied cyber science. This might well be addressed by building criteria into existing programs that accredit schools at all levels.
- A taxonomy of cybersecurity roles and the specific skills that practitioners must demonstrate to claim competence in each specialty. These roles should not be limited to those whose principle function is security. Software engineering, for example, is critical to effective cybersecurity.[8] The model must include the skills needed for cyber defense and building resilient systems rather than the unobtainable goal of preventing all cyber intrusions.
- A robust network of professional credentialing entities that maintain and administer independent professional accreditation processes for one or more area of specialization. That credentialing must, at a minimum, include:
    1. Knowledge-based testing;
    2. Successful completion of a period of internship under the tutelage of a credentialed professional to allow the individual to demonstrate his/her proficiency at applying relevant knowledge;
    3. Requirements for continuing education and periodic retesting;
    4. A code of ethics; and
    5. A process for de-certifying individuals who either fail to maintain their proficiency or who have otherwise failed to meet professional standards.
- An expectation that everyone who touches the cyber infrastructure, from senior executives to everyday users, will demonstrate cyber acumen.

The cybersecurity workforce issue is not a greenfield. A number of organizations are addressing pieces of the problem. The challenge for the next administration is to use its authority and resources to accelerate and harmonize those efforts, align skills toward current and future needs, and to fill gaps.

Where we need to go

Realizing this vision will depend on the initiative of the private for-profit and not-for-profit sectors. Education and training are not inherently Federal Government functions and the development and promulgation of standards and credentialing regimes has historically been under the leadership of private, voluntary groups. Presidential leadership can, however, be a catalyst.

While the public sector and the nation as a whole are largely reliant on the private sector both for the provision of cyber infrastructure and the education and training of the workforce, the Federal Government plays a critical role in several ways:

- Developing models in the way it manages its own workforce; including setting

[8] Imagine in the 21st century offering a curriculum in civil engineering without a course on stress and loading.

requirements for rigorous professional credentials[9];
- Investing, strategically, funds available to build the government's cyber workforce to support hands-on learning;[10]
- Creating and/or funding education and training to address the skills that are unique to the government and sharing the knowledge gained from those investments; and
- Supporting development of and adopting technology-based tools that can assume some of the cybersecurity functions for which humans would otherwise be required.

The following charts illustrate where we are and where we need to go.

Driving Change

Assessing the need against current threats

Effective security and response against highly advanced cyber threats requires a current understanding of what adversaries are capable of and enough experience with events that drive security work (this is especially true with highly targeted attacks) to become familiar with observables, decision making, and the application of knowledge. It is time to assess and prepare individuals to ensure they are competent, prepared, and capable of making the decisions day-to-day and during emergencies, despite the distraction or distress created by a constantly shifting adversarial threat. Considering the magnitude of the current challenge and emergence of newer models to better address cyber risk shifts the required competencies towards more technical hands-on skills.

Cybersecurity programs lack balance

Balance is the necessary element for a capable defense in today's world of targeted cyberattacks. Attacks will continue to occur and it is foolhardy to assume that organizations can always stop them. Recent well-publicized attacks, such as the Office of Personnel Management (OPM) compromise, once again demonstrate the criticality of enhanced detection capability, quick response and flexible mitigations. An organization must possess an appropriate number of well-trained and skilled staff serving in defense critical roles to ensure success. Their numbers matter if for no other reason than to investigate and adequately respond to multiple indicators of compromise and suspicious behaviors while learning and rapidly shaping their defensive capabilities to deal with the next intrusion attempt. We call the right role mix in sufficient numbers the critical mass for a functional active defense.

The global community lacks a ruler to provide an organization the ability to measure their existing staffing and requirements to determine if they are properly balanced and to take advantage of existing talented personnel. An organization that is overly tilted towards architecture, policy, and compliance roles will need a dedicated plan to obtain and develop the necessary technical skills to field an active defense team. Defender roles in the context of achieving an active defense are more technical in nature requiring more hands-on skills than legacy cyber prevention-focused security programs. For an organization to measure themselves

[9] Department of Defense Directive 8570.1, Information Assurance Training, Certification and Workforce Management, issued in 2004 was a first albeit flawed effort to link professional certifications and cyber roles.
[10] Programs like capacity grants under the National Science Foundation's Scholarships for Service.

against the ruler their staff must demonstrate competence in performing critical tasks and using relevant categories of tools. To accommodate the ever evolving security postures of organizations each defender role and its critical tasks were broken into three levels: Novice, Journeyman, and Master. Thus, organizations that can identify the critical roles, understand the critical tasks for each role, and can identify their personnel appropriate to the category and skill level represented within this paper can measure their security posture and move to a more mature security status. Ultimately, it takes highly trained and empowered defenders to counter well resources and determined adversaries. Defense is a worthwhile albeit difficult goal. However, we believe that defense is doable. This new paradigm is comprised of hard won realizations that attackers can't be kept out of systems requiring organizations to be able to prepare, detect, and defend systems.

Requirements of mounting a credible cyber defense

Proper balance is the necessary element of a capable defense in the face of targeted cyber attacks. It is impossible to stop all attacks. Organizations must have the security maturity to realize that an adversary breaching security at the perimeter of the network is not the measure of failure. Security metrics relating to number of scans or pieces of malware blocked by firewalls and endpoint solutions also lend to misleading and highly inflated numbers. Instead, organizations must reach a point where it is expected that they can identify intruders without over relying on third party notifications, respond to them appropriately within friendly networks, learn from the threats in an effort to stay agile and prioritize efforts, and apply that knowledge to achieve long-term security. To do this requires appropriately manned teams of well-trained and empowered staff serving in vital defense roles. While this has historically been the goal of many security teams an issue exists in determining common terminology, finding personnel internal to an organization that already possess the right skills but are in the wrong roles, and in properly defining roles for the defense teams. The aim of this project is to illuminate those gaps and alleviate these issues by focusing management's attention.

In pursuit of this project we have designed a ruler of key defender roles that will allow organizations to measure their existing staff against specific competency requirements and measure role to task alignment. Role to task alignment is a necessary view as many organizations tend to over apply their few talented people to solve security problems in other areas than detection and response. How many times have these skilled people been used for testing and assessment tasks or asked to solve technical support challenges? The measurement of ground-truth technical staff utilization will empower these organizations to balance requirements to ensure they are prepared for the current and emerging threat landscape. The defenders' roles and measures for success are categorized in the context of an active defense. This category of defense and its conceptualization in context of other actions can be understood best in the Sliding Scale of Cyber Security.

The roles that are associated with an active defense capability include analytical, investigative, engineering, and operating focused positions. For some organizations, it may be sufficient to collapse two-competency models (engineering and operating) into one role. The authors have defined roles based on unique competency models with accompanying measures. We need a taxonomy of cybersecurity roles and the very specific skills that practitioners must demonstrate to claim competence in each functional role. A first draft of such a taxonomy is contained in Appendix A. This framework is intended as a ruler against which leaders can measure the cyber-

competence of their own organizations.

Professionalizing Cybersecurity

Maturing the nation's certification system

Calls for greater rigor in the market for certifications has received some incremental progress since the Cyber Commission for the 44th presidency made its recommendations in 2008. Their recommendations focused on the creation of a governance body initially based on a federated model, which would develop and administer certifications in two or three specialty areas and evaluate whether some/any existing certification programs meet its standards. The organization was suggested as a not-for-profit. Such a board was to assemble but efforts to collaborate with the commercial marketplace were quickly stalled and the board focused on research into the field of cyber competencies as a resource for future efforts. Such as organization should work with the following entities to achieve future progress:

- Major private sector organizations that employ cybersecurity professionals;
- Universities with major cyber education and research programs; and
- Key Federal Government agencies[11]

Developing Cyber Awareness in the Non-Cyber Workforce: Cyber Acumen

Cyber has pervaded every part of our daily lives. It serves to improve our productivity, increase our connection to the world around us, and provides access to basic services. Companies throughout the world are taking advantage of this transformation and branching into new markets, governments are digitizing their services and providing more efficient and personalized interactions. As the data has moved into this digital world so has the crime, espionage, and other nefarious acts and actors. Study after study shows that today's world is one where enterprises work hard to stay ahead of these adversaries, and are very often unsuccessful. Improving our success rate will require that everyone, not just whose primary function is cybersecurity, have a basic level of understanding and awareness much as one does not need to be a health professional to mitigate health risks.

Cyber Awareness is a key part of today's strategy for including the users and their behavior in the overall security of the systems and applications in use throughout the US Government. It has long been held that "the first step in changing the culture is to build wider understanding of reasons to change."[12] This belief created the need for an awareness campaign to explain the importance of cyber security and the role of users and consumers. As a result, general awareness has been a part of National Initiative for Cybersecurity Education (NICE) since its inception. In the workplace, general awareness typically includes annual training and can include on-the-spot efforts focused on specific threats such as phishing exercises for employees. These awareness efforts have been a part of the comprehensive national cybersecurity initiative since 2008. However, there is not consensus on the value of the national campaign and its efforts to increase

[11] Since this would be an oversight/advisory group, not a board of directors with fiduciary responsibilities, we presume that it will be possible for government officials to participate

[12] (Mueller October 2013 Building a culture of cost consciousness_ DAU Press).

general consumer awareness. Additionally, criticism remains of the effectiveness of awareness training for employees including the annual training the federal government requires of its workforce. Bruce Schneier, a recognized expert in cyber security is among the strongest critics of the value of awareness training. In his March 23, 2013 blog Schneier on Security he is clear about his beliefs of the value of training. "I personally believe that training users in security is generally a waste of time, and that the money can be spent better elsewhere. Moreover, I believe that our industry's focus on training serves to obscure greater failings in security design." (Schneier on security march 23, 2013) Schneier acknowledges that his opinion is his own and that the debate about utility and value of general awareness continues. Core to this debate is the question, 'Is awareness enough to help decision makers be more effective in juggling their responsibilities of meeting mission and performance demands in a digital world where the environment includes criminals, hackers, and other actors who are intent on disrupting operations, gaining proprietary, confidential or classified information, or influencing or altering the very data stores that feed business processes or decision making?'

It is time to move from awareness to acumen

Acumen is defined as "the ability to make good judgments and quick decisions, typically in a particular domain".[13] Cyber acumen is a needed competency that enables the application of a basic understanding of cyber practices with business and mission activities. Many domains have begun to recognize the need for acumen in business and technology in order for their workforce to be successful. Auditors are now encouraged to develop business acumen; Human Capital Officers are now encouraged to develop acumen in the areas of information technology. OPM established a business acumen Executive Core Qualification as a part of its Senior Executive Service transformation more than 20 years ago. OPM defines business acumen as the ability to manage human, financial and information resources strategically. In the 21st century environment we operate in, this ability is necessary, but arguably insufficient.

Cyber acumen requires more than just strong management abilities in these three domains: financial, human capital and technology. Cyber acumen is the ability to manage the business activities which are now encapsulated in technology in an environment where a variety of digital threats must be handled simultaneously. It is not the basic programmatic management activities covered in business acumen where limited resources are allocated across prioritized requirements, rather it is the constant focus on succeeding in these programmatic activities in the fluid environment where many variables must be understood but cannot be managed.

Elements of this include a deep understanding of how and where cyber is woven into the mission space of the organization or function. Demonstrated ability to operate in the complexity that exists in cyber, both in the evolution of the technology and user dimensions as well as the adversarial environment. It includes a recognition of the threats and opportunities cyberspace presents to mission accomplishment. Supports an understanding of the limitations of analogies from the physical domain balanced with the need to not invent everything new, but rather know when to adopt solutions and analogies from other domains. This is not a specialization, nor a skill that only fits in the engineering organization, rather cultivation of this acumen on a broad scale would be beneficial.

[13] (Webster online)

Several organizations have begun to recognize this need. Programs such as the US Naval Academy have recognized the inherent risks of operating in this contested space and have added an introduction to cyber security into the core curriculum that every midshipman must take. They introduce each student to the basic principles of cyber security including key protection and defense methods and importantly expose their students to the concept of cyber operations and the thought processes and methods used by adversaries.

Leaders in both the public and private sector serve many important purposes; among them are providing focus and setting priorities that drive how much time and attention managers will spend on particular topics. Increased acumen in cyber will result in better choices in this area. Creating a leadership competency will help current and future leadership be more effective as they manage the challenges they are facing whether it be transforming legacy technologies or increased demand for mobile service.

Recommendations for Action

In order to achieve the Vision outlined in this paper, the Administration should adopt the following recommendations:

For the short term:

1. Adopt the concept of "cyber acumen" for the Senior Executive Service (SES) as part of the SES Executive Core Qualifications (ECQ). Currently, ECQ 4: Business Acumen includes a technology management component and states "Ensures access to and security of technology systems." The establishment of new ECQ specifically for cybersecurity within the SES will ensure cybersecurity and risk is management appropriately;

2. Move the workforce operation currently within the NPPD which resides within the Office of Cybersecurity and Communications (See https://niccs.us-cert.gov/home/about-niccs.) to the National Institute of Standards and Technology (NIST) where the NICE initiative is being lead. There is no statutory authority for the function NPPD is performing and this causes confusion within and outside of the federal government with NIST who is the statutory led;

3. Dedicate the appropriate resource levels to support cybersecurity education, training and public awareness programs through the Department of Commerce and the NICE initiative specially to engage minority candidates not typically represented in STEM programs with specific encouragement to private sector to match the federal government funding levels with the President convening and launching this combination of efforts; and

4. Recruit one federal government cybersecurity employee per year by the President with a personal call to the high-value candidate to lead by example.

For the mid-term:

1. Adopt a system for accrediting training and education institutions offering programs in either theoretical or applied cyber science;

2. Adopt a taxonomy of cybersecurity roles and the very specific skills that practitioners

must demonstrate for competence in each specialty;

3. Adopt white-hat hacking courses including ethics at elementary and high school level supported by the federal funding provided at the state levels;

4. Develop specific veterans job recruiting program including an evaluation of existing programs to prevent duplication and expand the program(s) which are working well similar to the Department of Veterans Affairs contract management initiative for veterans.

For the long-term:

1. Develop a robust network of professionals and professional credentialing entities. This network of professionals could be established similar the "NET Guard" authorized in P.L. 107-296, Section 224, expanding the NET Guard to include cyber response capabilities, which at a minimum would include capabilities both within the government and private sector in support of disaster responses similar to a "first responder capability to protect the nation in the event of a large-scale cyber-attack.

APPENDIX A - A proposed taxonomy of critical cybersecurity roles and competencies

A working definition for "mission-critical roles" comes from the CCS[14] research on scenario-based competency modeling: "functional job roles that bring the necessary know how, competencies, and practices to accomplish the mission of an organization."

Job	Tasks	Consequences of Failure to Perform
Security monitoring and event analysis	Identify indicators that show an incident has occurred and initiate swift response, differentiating between those incidents that represent impotent attack vectors and those that need to be analyzed in-depth by the incident responders. Many other tasks are performed by the security monitoring and event analysis staff, but the ones described here are the critical tasks for which skills are in very short supply.	Failure to identify new attacks that mimic old, impotent attack vectors provides savvy intruders with an easy vector to bypass defenses.
Incident responder in-depth	Implement proactive measures to contain the incident, including isolation, characterization, reverse engineering, assessment of capability and activity of malicious software that has been found on agency systems, identification of intruder local changes/suspect interactions, triggering of targets to evoke malicious behaviors, and development and deployment of eradication tools. Only 2%–10% of all malicious software needs to be put through this deep analysis; the remainder will be cleaned with anti-virus tools using current and updated signatures. However, the 2%–10% constitute the most dangerous payloads.	Malicious software will be able to spread through agency systems by burrowing deep and maintaining control as well as by leaving back doors for unauthorized access at will. An unacceptable duration of attacker free time will result in freedom of movement and action. Lack of understanding of attackers and their tools (advanced malware) will undercut the defensive efforts of incident responders and threat analyst. Attackers can reuse tactics and tools to re-attack or maintain their control over systems for long periods, taking and changing data at will. Anomalous and malicious behavior by insiders will go undetected.
Threat analyst	Deploy deep and current knowledge of the attack surface, its most vulnerable and high value targets, and how its technical vulnerabilities may be exploited; maintain up-to-the-minute situational awareness on what malicious actors are using and targeting; and develop techniques and custom tools to detect local changes, identify suspect interactions, watch and respond to what malicious actors are doing. More advanced teams also are able to understand the attackers' motivation, language, organization, and social behaviors, as well as group the threat actors logically to create effective profiles of groups, actors, and campaigns, thereby helping organizations become more proactive in their security posture and defense.	Freedom of action (including the exfiltration of sensitive information), and undermining of the defender's ability to act. Well-embedded adversaries can actually resist defender efforts as they are privy to instructions and can work to stay a step ahead of observed defender actions. Further, not understanding the current threat landscape and exactly how the attacks work in technical detail will lead to insufficient defenses against those vectors and will unnecessarily raise costs.

[14] Council on Cybersecurity now a program under the Center for Internet Security: Mission-Critical Roles from the HSAC CyberSkills Report.

APPENDIX B - Excerpt of Mission-Critical Roles from the HSAC Cyber Skills Report

This work and practical implementations of cyber defense programs has led to an initial recognition of the types of roles needed:

- Threat Intelligence analyst
- Intrusion Analyst
- Incident Responder
- Forensic Analyst
- Malware Reverse Engineer
- Technical or Team Director

Levels of competencies & role descriptions:

Staff can be measured to fall within three levels of competency in each job role. The levels can span from beginners to expert performers, but for the purposes of measurement we will focus on competent, expert, and master levels. These levels are in line with previous work by a research not-for-profit, NBISE, which stated, "What is optimal performance differs greatly between beginners, or those merely proficient in methods and tools, and the skilled competent or expert performers."[15]

Threat Intelligence Analyst

A Threat Intelligence Analyst is responsible for establishing intelligence requirements, formulating a collection plan, collecting, analyzing, and disseminating information about the organization's threat landscape to the appropriate teams. The members that fill this position should have a mixed background of technical and non-technical skills in order to understand the threat and the context around the threat including any geopolitical or business operations considerations when dealing with advanced adversaries. It is also paramount that Threat Intelligence Analysts understand the difference between generating and consuming intelligence. Generating intelligence can be conducted based on a mix of internal data collected from incidents and threat interactions and should be formalized in a manner to be shared with peers in the community. Consuming intelligence requires the analysts to understand their organization's intelligence requirements, as well as people, processes and technology to make accurate assessments on the threat intelligence and the applicability to the organization. There are a number of organizations that provide threat data and make it available. Threat Intelligence Analysts should be able to filter through the vast amounts of information to find the high fidelity information that is relevant to the organization and its security personnel. More senior Threat Intelligence Analysts should also be able to identify deficiencies, communicate threat intelligence to decision makers effectively, and help foster partnerships with peer organizations.

[15] The National Board of Information Security Examiners (NBISE), MCRP Final Report. The Department of Homeland Security (DHS), Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council comprises leaders from state and local government, first responder communities, the private sector, and academia. Source: http://www.dhs.gov/homelandSsecuritySadvisoryScouncilShsac

- Competent
    - Understands intelligence collection requirements
    - Can accurately collect information when tasked
    - Capable of leveraging open source tools such as Google to find threat intelligence reports and research identified threats
    - Identifies useful indicators of compromise (IOCs) to pass to other active defense roles
- Expert
    - Understands the organization's people, processes, and technologies intimately
    - Capable of seeking out and collecting information related to current and emerging threats that the organization does or will likely face
    - Takes full advantage of multiple tools (open source or proprietary) to collect and analyze the information required
    - Can create new IOCs relevant to the organization from internal or external information sources and effectively disseminates them to the other active defense roles
    - Initiates briefings on adversary tactics, techniques, and procedures to other active defenders for the purpose of identifying and learning how to respond to threats
    - Understands the organization's critical information that requires protection
- Master
    - Identifies and executes on opportunities to expand tools and tradecraft for the organization's threat intelligence capabilities and personnel
    - Can effectively communicate the threats and their impact on the organization to decision makers in a manner that guides appropriate actions and investments
    - Identifies opportunities for increased communication and sharing within the organization and amongst its peers

Intrusion Analyst

Intrusion Analysts are those individuals who hunt throughout their organization to detect and initiate analysis on threats inside the organization's environment. These personnel take full advantage of the data available including network and system logs, network topologies and data flows, and alerts generated from the security architecture to find the threat, remediate it if it is incidental or minor, or make recommendations to initiate incident response procedures in the event of a more serious compromise. During incident response procedures the Intrusion Analysts are also responsible for maintaining situational awareness and guiding incident responders in their efforts to scope and contain the threat. Senior intrusion analysts can also help make recommendations to the architects of the network to better shape the network into a more defensible system.

- Competent
    - Actively monitors and responds to alerts from the security architecture
    - Understands how to review security events to be able to differentiate between normal activity, false positives, and events requiring immediate attention
    - Analyzes alert TTPs and indicators against previous activity
    - Establishes case/ticket in the organization's incident response system
    - Communicates incidents to the appropriate internal groups

    - Escalates incidents requiring mitigation to the incident response team
    - Queries security architecture to collect additional information related to the alert
    - Gathers target profile information (people, technology, process)
    - Understands the security tools and processes at their disposal to respond to alerts
- Expert
    - Understands the organization's people, processes, and technologies intimately
    - Conducts initial triage of the incident
    - Understands network protocols and system generated logs
    - Analyzes alert TTPs and indicators against intelligence sources
    - Deploys new intrusion signatures to detect additional activities related to the alert
    - Uses target profile information to establish initial risk to the organization such as susceptibility to attack, value of asset, process, person
    - Performs analysis of network traffic, intrusion alerts and system logs
    - Effectively communicates with peer active defense roles and the larger organization
    - Understands the normal behavior profile of the network
- Master
    - Identify deficiencies in the organization security architecture and policies
    - Developments custom intrusion signatures to detect and mitigate additional activities related to the alert
    - Effectively communicates with peer active defense roles, the larger organization and external organizations
    - Develops process and procedures for intrusion analyst roles, policies and processes
    - Provides expert analysis of network and system information and logs for advanced adversary TTPs

Incident Responder

Incident Responders are the front line defenders when a breach occurs. Not all compromises on a network require incident response. However, in the event that decision makers initiate incident response procedures these personnel ensure understanding of the scope of the problem. In practice, Incident Responders are guided by the other security personnel in the organization to infected systems and by their own analysis of the threat's indicators. Primary goals for incident responders include scoping the threat, collecting forensic evidence with volatile evidence prioritized, and working with architecture teams and system engineers to contain and remediate the threat once it is understood. More senior incident responders help posture the organization ahead of an incident to better prepare the planning, procedures, and response efforts. A significant majority of work done for any incident is done during the planning stages. This reduces the cost of incident response while ensuring a more efficient response. Incident responders' role in these preparations and in coordinating training and understanding between other active defenders cannot be understated.

- Competent
    - Tasks security architecture and personnel for focused collection
    - Executes the incident response process
    - Functions as the incident point of contact

    - Understands the security tools and processes at their disposal to manage incidents
    - Effectively manages the incident response system and associated organizational change management processes
- Expert
    - Understands the organization's people, processes, and technologies intimately
    - Maintains effective relations with internal business stakeholders
    - Performs incident hotwash for lessons learned
    - Establish an initial timeline of the incident and ensure all information is documented
    - Determines the scope of the incident
    - Communicate incident information to maintain situational awareness
    - Ensure all security solutions are up to date against the threat(s) and all associated TTPs and IOCs for this incident
- Master
    - Modifies the incident response plan to address changes in the threat landscape
    - Establishes relationships with external partners to address industry or sector specific threats
    - Effectively communicates with peer active defense roles, the larger organization and external organizations
    - Identify deficiencies in the organization security architecture and policies
    - Coordinates, prepares for and briefs senior business stakeholders on risk to the organization, impacts and lessons learned

Forensic Analyst

Forensic Analysts interrogate collected forensic evidence to identify the impact of a compromise. Understanding the impact should include answering questions such as the what, where, when, and how of the compromise. These analysts prioritize uncovering the truth of the investigation which ultimately leads to better understanding the threat itself. Traditionally, forensic analysis has been a back shop function of security which took place over the course of months instead of directly complimenting the current security efforts. Forensic Analysts that are taking part in an active defense role should work to get the most viable data out of the evidence as quickly as possible for the purpose of injecting it into the security process. With this data incident Responders should better understand the scope of the threat, Malware Reverse Engineers should better identify different variants of malware in the organization, and intrusion analysts should more accurately prioritize their investigative look into the organization. The goal of the Forensic Analyst should be prioritized on the security of the organization and not on the traditional thought process of legal systems and prosecution. More senior Forensic Analysts should be able to break down cultural and technical barriers to communication between active defenders.

- Competent
    - Establish points of contact for all sites and or facilities where physical access may be required
    - Identify users and administrators that may have access to the systems or information in question
    - Conduct an initial triage of the system
    - Capture a forensic image of the system

    - Understands chain of custody and safe evidence handling
    - Understand server and workstation communications and file systems
    - Understands the placement of forensics tools and capabilities
    - Understands how to capture a memory image
- Expert
    - Extract indicators from identified artifacts to search the enterprise for additional suspicious and/or related activity
    - Identify suspicious malware on hosts
    - Understands how to review security events to be able to differentiate between normal activity, false positives, and events requiring immediate attention
    - Detailed knowledge of system and application logging capabilities
    - Performs system log analysis looking for suspicious behavior
    - Understands how to conduct meetings with HR, Legal, Security, etc. on the status of the investigation
    - Understands how to translate threat data into a consumable indicator of compromise
    - Understands how to isolate or remove affected systems from the network
- Master
    - Understands how to perform memory image analysis
    - Understands how to implement clean up procedures
    - Understands the basic jurisdictions of law enforcement, available capabilities to aid in the investigation, and details for contacting appropriate law enforcement agency
    - Understands how to detect secondary and tertiary indicators of compromise

Malware Reverse Engineer

Threats are not always malware based but an overwhelming majority of threats faced today are enabled by malware or focused on its use. Malware Reverse Engineers should be able to analyze the malware in a timely way to support the hunt for it and its variants throughout the organization as well as understand its capabilities. Understanding malware capabilities can help prioritize defense and incident response efforts especially when multiple threats are being faced simultaneously. These analysts should be keenly aware of the organization's priorities and valuable assets to help guide informed decisions and remediation efforts against threats targeting these priorities or assets. Senior Malware Reverse Engineers should be capable of identifying opportunities for more automation of the process and execute on these opportunities to scale the efforts of their team to maintain timely analysis in an evolving organization.

- Competent
    - Performs static analysis of malware artifacts to collect metadata
    - Analyzes malware artifacts using automated solutions (static and dynamic)
    - Searches available intelligence and open sources to identify the activity or relate it to exiting IOCs or TTPs
    - Identifies file format using tools or static analysis
    - Understands operating and file systems
    - Understands network protocols

- Expert
    - Detailed knowledge of various file formats
    - Performs dynamic analysis of artifacts
    - Understands the use of debuggers, disassembly and hex editors
    - Understands assembly language
    - Modifies artifact code to force execution (circumvent passwords, strings, phrases)
    - Understands analysis defeat techniques (VM detection, encryption, debugging detection)
    - Creates custom programs to analyze malware artifacts
    - Identifies indicators of compromise for mitigation and signature development
    - Provides mitigation recommendations
    - Performs network traffic analysis of malware artifacts
    - Identifies malware features, functions and command structure
- Master
    - Understands how to defeat analysis detection techniques
    - Modifies artifact code to defeat encryption routines
    - Performs file analysis to identify encryption routines
    - Develops signatures or capabilities to detect indicators of compromise

Technical Director

Those individuals filling the Technical Director role for an organization's active defense efforts should be fully aware of their organization's operating environment to include the people, processes, and technology present. This includes an understanding of the current security architecture of the organization as well as the efforts and tools leveraged by the active defenders. This position is responsible for collecting, coordinating, and communicating the lessons learned from interactions with the adversary. The purpose of this effort should be to help the organization and its architecture evolve over time into a more secure state. The Technical Director is also responsible for ensuring that the active defender roles work effectively together and that these efforts are communicated properly to decision makers in the organization.

APPENDIX C - Organizational Maturity Model

Organization maturity continues to be ad hoc despite efforts to provide resources to help identify roles and competencies to inform the design of workforce strategies.

Maturity Level I – Pre-job definition

The organization can identify its mission requirements, joint capabilities, workforce composition and goals and can relate these things to Job definition or classification.

Maturity Level II – Job's defined (JTA)

These organizations have begun to develop competency models (JTCA) are able to select performance assessment and skill analysis tools to inform their workforce development plan.

Maturity Level III – Existing assessment instrument

These organizations conduct skill profiling and have identified standards for qualification or

certification and may invest in the development of measurement instruments to assist in achieving some level of workforce qualification. This information provides input to a workforce development plan.

Maturity Level IV – Existing certification

The use of validated measures and data analysis to identify skills and verify workforce development plans.

Maturity Level V – Education and Training

These programs have mature tools to assess the existing workforce and evaluate job candidates. Workforce plans are well understood and are improved with feedback based on performance and needs.

GLOSSARY

Competency: An Observable and measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual need to successfully perform an activity

Mission-Critical is used to define the importance of the work to be performed by the cyber functional role as being critical to the defense of an organization/agency's information systems. (CCS MCRP Final Report)

Functional Job Role is a label given to a category or classification of job roles based on their sharing a significant number of common goals (i.e., functions). (CCS MCRP Final Report)

Job Role is a label given to a category or classification of job titles based on their sharing a significant number of common responsibilities or job duties. (CCS MCRP Final Report)

K*nowledge* is defined as the understanding of a concept, strategy, or procedure. Thus, knowledge is measured by depth of understanding, from shallow too deep. Knowledge is therefore independent of task performance. Knowledge is identifiable by the capacity to encode, recall, or associate information, independent of context. For example, organizational knowledge is required to "Understand what is important to the organization and what is mission critical." (CCS MCRP Final Report)

Skill is defined as the reliable application of knowledge in the accomplishment of a task to achieve desired outcomes. Thus, skill is measured by the degree of reliability, from inconsistent too consistent, in performance of a task. Skill is always task specific and context specific. Skill is identifiable by statements of accomplishment, such as "Establish plan for secure storage and transmission of customer data." (CCS MCRP Final Report)

Ability is defined as a mental or physical capacity to transfer or transform knowledge and skills for application to new domains. Thus, ability is measured by the extent of knowledge and skill transfer, from narrow too broad, typically assessed through the use of physical or intelligence tests. Abilities are task independent. Abilities include many forms of mental or physical manipulation (Guilford, 1956), e.g., dexterity, locomotion, memorizing, deducing, recognizing patterns, and planning. (CCS MCRP Final Report)

Encryption and Going Dark – Cutting through the Gordian Knot

John Nagengast

David Simon

Introduction

Since the emergence of publicly available, highly secure encryption algorithms in the 1970's, there has been a continuing debate, both within the United States and around the globe, on their use in supporting individual privacy and the protection of personal information versus the ability of law enforcement and intelligence agencies to lawfully access this information. There has been much debate and controversy over this topic, and recent events have highlighted the lack of a comprehensive policy on the use of encryption within the United States, and its international implications, along with a concise legal framework governing lawful access to encrypted information.

And while the government's mid-1990's efforts to recommend a method to embody lawful access through a system involving escrowed key (the CLIPPER Chip) is perhaps the best known example of the contentious debate between privacy advocates and the government, few encryption developments over the past 40 years have been devoid of controversy fueled by suspicion and differing agendas. Indeed, the Data Encryption Standard (DES), established in 1977 as Federal Information Processing Standard (FIPS-46) through a public process by the then National Bureau of Standards (now NIST) was controversial from the beginning. The algorithm that became the DES was originally called Lucifer by its developers at IBM Research, and appropriately referred to by some as the Devil in the Blue Dress. The National Security Agency, serving as the authoritative technical resource for the U.S. Government in the selection process, recommended several changes in the combinatorial logic (known as the S-Boxes) of Lucifer to both IBM and NBS in order to strengthen it against certain types of cryptographic attacks. This engendered suspicion in cryptographic research circles that NSA had put a "back-door" into the algorithm. The futile search to find this alleged back-door by academia and researchers actually significantly advanced the public knowledge of cryptographic design and analysis. DES encryption and its successors, Triple DES and the Advanced Encryption Standard (AES), were eventually adopted world-wide for protecting sensitive information in both Data-in-Motion and Data-at-Rest applications, along with the related hashing, key formation/exchange, and randomizer functions. However, the widespread adoption of encryption has only served to intensify the ongoing controversy over privacy, security, and lawful access.

While often characterized in terms of technology (e.g., a particular implementation of digital encryption), the underlying issues of encryption and 'going dark' can be described as the challenge of reconciling three aims:

- The desire by individuals (supported by most governments) for privacy in their communications and data transmitted across or stored on digital devices and networks
- The desire by government organizations to access the communications or personal data of individuals in support of law enforcement or national security (e.g., in pursuit of collective security)
- The desire by technology providers to develop and sustain the confidence of their customers in the robust security of their products (driven by their dual responsibility to customers on the one hand and company shareholders on the other). This desire is particularly acute for companies doing business across differing legal regimes where the balance struck between privacy and collective security is uneven and often unpopular with individual citizens.

Taken individually, each of these three aims can be viewed as a laudable goal. Taken in sum, an unqualified commitment to one of the aims necessarily makes it more challenging to achieve one or more of the other two. Further, the dynamic nature of technology and its creative application to myriad tasks by millions of users greatly increases the difficulty of striking and sustaining a particular balance over time. Keeping up with this ever changing landscape has always been a challenge for the conduct of lawful surveillance by law enforcement or intelligence agencies. This is generally referred to by the law enforcement community as "going dark". Encryption is but one component of this challenge.

The Apple versus FBI Debate

A prime example of the passions engendered by the encryption topic is the debate being played out in public and in the courts over FBI efforts to recover the data on the iPhone used by Syed Rizwan Farook, one of the perpetrators of the San Bernardino, CA terrorist attack in December 2015. Apple CEO Tim Cook argued that providing technical assistance to the FBI in recovering data from the phone by the method the FBI has suggested would undermine the whole security foundation of the iPhone, and endanger personal privacy globally (not to mention Apple's market position), teeing up a perceived collision between individual security, collective security and Apple's pursuit of global markets. The instant legal confrontation between FBI and Apple was obviated (but not resolved) when the FBI hired an unknown party who was able to defeat Apple's security mechanisms and unlock the phone, and the Justice Department dropped its court proceedings against Apple.

While this is certainly an important part of the encryption puzzle, recovering the data on a client device, whether it is encrypted or not, is only one part of the issue. In fact, the energetic food fight over retrieving the data on a dead terrorist's phone in the physical position of the FBI and the polarization it has engendered may actually be a distraction to addressing the larger set of issues in a thoughtful and balanced way. It is absolutely ironic that all of this collective energy has being expended on a relatively small portion of the overall cybersecurity and encryption equation. It appears that Apple has done an excellent job of embedding data-at-rest security into its most recent devices while locked; however, this data is certainly at greater risk (as with any mobile device) when the phone is unlocked by the legitimate user or a particular application is invoked (either of which automatically decrypts the data stored on the device) and connected via the wireless network to the Internet at large.

Putting Encryption in Context

While a complete and comprehensive "solution" that satisfies all sides in the debate may never be possible, it is useful to break the problem set into manageable portions. Much confusion is caused by the different ways encryption can be used for protecting data-in-motion and data-at rest, and the terminology involved. In particular, many privacy advocates frequently use the somewhat pejorative term "back-door" when discussing encryption, without defining what they mean. For example, where user or enterprise data is stored in the cloud and encrypted for security, the cloud provider will necessarily provide several ways of backing up and recovering/decrypting the data in case of failure. No user wants to risk losing their data due to a failure anywhere in the system, including forgetting a password or the loss or theft of a client

device. Thus the ability to recover data is an essential element of the security design, and not a "back-door", i.e., an unacknowledged feature allowing surreptitious access.

Any security design, whether employing encryption or other measures, will always have vulnerabilities of some sort. The question then becomes is the risk of the vulnerabilities being exploited sufficiently low given the application. Like all other aspects of digital design, the encryption schema and other security measures being contemplated involve a series of tradeoffs. The security design must fit the way the device will be employed and not have unacceptable consequences, such as greatly reduced battery life, a significant increase in device size and weight, or unacceptable performance in the basic functions and applications of the device.

In the situation of an unlocked mobile device (or any other client device) connected to the Internet, the threats to the data stored on the device include international crime syndicates, adversary intelligence agencies, terrorist groups, and the full collective of hacker and hacktivist groups around world, not just a US law enforcement agency which has the device and a valid probable-cause warrant. Further when discussing the encryption paradox, the continuing evolution of the underlying technology must be considered. While current mobile devices have become more and more capable as end-point devices, and are largely replacing personal computers and laptops for many users, this is likely to change over the next several years at the strong trend to virtualization and cloud continues. Mobile devices will more and more become portals to cloud based applications and information, with individual user and enterprise data stored in the cloud as a matter of course, enhancing capability, flexibility, security and privacy. In the overall security equation, moving all the data off the mobile device and into the cloud provides significant advantages, and in effect will moot the instant issue between Apple and the FBI over lawful access to data on the device. Of course, all data moved between the device and the cloud will be encrypted while in transit, and the data stored in the cloud will be separately encrypted while at rest, presenting other challenges and issues for lawful access.

For discussion purposes, we would identify the components of the problem as follows:

1. Establishing the value proposition:

- In the absence of a shared commitment to pursuing solutions that deliver individual privacy protection, the ability of government(s) to pursue lawful access for legitimate collective security purposes, and the ability of companies to set and meet global expectations for their products, no particular implementation will end the controversy

2. Going Dark:

- New forms of communications technology, e.g., fusion of cellular and Wi-Fi communications via 5G/LTE.
- Evolution of social media allowing new forms of communications.
- Locating and accessing communications or stored information of specific individuals or enterprises in a virtual, cloud based environment.

3. Encryption:

a. Data at Rest

- Full Disk/Memory Encryption of Client Devices
- Full Disk/Memory Encryption of Servers/Hosts

- Encryption of Cloud Data in a Virtual Environment

b. Data in Transit

- Peer-to-Peer client applications with embedded encryption
- Network layer encryption between Client Devices or Client to Server Scenarios
- VPN Encryption between Enterprise Enclaves
- VPN Encryption Client to Cloud

Overall Trends in Technology, and Implications for Going Dark & Encryption

First and foremost, one of the dominant trends in technology is the move to a cloud-based virtual environment for the hosting of applications and data. Individual or enterprise users will securely store and process their information in virtual containers in the cloud, providing flexible communications and computing capabilities on-demand as required. Virtual environments provide better overall performance at lower cost, and can be made highly secure and resilient for the full range of applications. Open source virtual environments such as OpenStack and the Docker/Open Container Initiative are being widely adopted by cloud service providers for both public and private clouds because of their inherent performance, cost, and security attributes over traditional hardware-based dedicated computing platforms. With these approaches, each application or data set can be deployed in its own protected computing environment, surrounded by an individual security policy and boundary. Stored data will be automatically encrypted as an integral part of the security environment, and further protected with strong authentication, sophisticated intrusion/malware detection, and comprehensive transaction logging at the individual container level.

As the enabling infrastructure for end devices evolves, so will the end devices themselves. With the advent of 5G/LTE wireless capability coupled with the integration of Wi-Fi capability into a seamless wireless environment, the available bandwidth for end-devices will dramatically expand. His will allow the compute and storage capabilities to move into the cloud, making the end-devices considerably simpler and less costly. All user data will be securely stored in the cloud as described above, with connectivity between the end-device and the data or application container in the cloud encrypted at either the application or network level.

We also can expect with high confidence that various forms of social media will continue to expand and evolve, as well as new applications emerge for mobile devices. This will be coupled by the ubiquitous use of strong authentication and identity management services, engendered by the spread of mobile devices for electronic payment (e.g. Apple Pay, Android Pay, etc.), digital wallet, and other on-the-go payment and financial applications.

As a result of this evolution, the law enforcement and national security community will continue to be challenged to stay ahead of, or even keep pace with, the technology curve. The good news is that the trend to cloud-based storage of data, with the necessary back-up and resiliency to eliminate single-points-of failure, will ameliorate some of the current concerns about gaining lawful access to encrypted data on the end-device. At the same time, identifying and locating the relevant data under a warrant in the cloud, or even getting enough information to support issuance of a warrant or other lawful means, will be more considerably more complex. Also, the challenge of identifying and accessing encrypted data in motion will continue to expand rapidly, particularly in the over-the-top, peer to peer space. Meta data on the communications will continue to be available, as the underlying transport networks cannot function without it, but locating and interpreting it will be orders of magnitude more difficult.

What all this means is that an unprecedented level of cooperation between law enforcement and the technology providers will be required to provide lawful access in the future, bounded and supported by a legal framework that carefully balances the three factors cited earlier: individual privacy in their communications and data; governments access to the communications and data for collective security; and the desire of technology providers to develop and sustain the confidence of their customers in their products' security.

Moving Towards a Pragmatic Strategy for the Global Marketplace

Perhaps the biggest inhibitor in finding common ground in the encryption and going dark challenge is the lack of a clear and relevant U.S. policy and legal framework, as evidenced by the Apple/FBI legal debate. Given this situation, technology companies are essentially put in a no-win position when asked for assistance by national security or law enforcement authorities, conflicted between their desire to protect their reputations of upholding their customer's privacy and to be successful in the global marketplace (and the anticipation of like requests by other governments), and their desire to help in legitimate efforts to thwart criminal and terrorist activities, either because they believe it is the right thing to do, or being legally compelled which gives them top cover.

Recommendations on Encryption and Going Dark

The upcoming change in Administrations will allow a fresh start with the various factions in the private sector in attempting to address these issues. To be effective, any US policy and legal framework must be developed in the context of the global environment and a US strategy for international cyber security. Accordingly, we offer the following recommendations:

1. The President should clearly articulate the governing principles for US and international cyber security, along with attendant US National Policy on Encryption and other relevant security technologies as they relate to the alignment of individual security (to include privacy concerns), collective security (to include law enforcement concerns), and economic vitality. This policy should support the use of strong encryption for privacy and security while specifying the conditions under which assistance from the private sector for lawful access to data will be required, along with the legal processes for obtaining such assistance.

2. Working in collaboration with the leading technology and security service providers, internet service providers, privacy advocates, and in consultation with key allies, the President should draft appropriate legislation to submit to Congress for consideration in implementation of the National Policy. While legislation will not have a direct impact on foreign government determinations, it should be consistent with US strategy to effect a global regime for the alignment of individual security, collective security and economic vitality interests.

3. In keeping with the trend to cloud-based applications and data storage accessed from mobile devices, the President should task NIST to work with encryption experts, technology providers, and Internet Service Providers to develop standards and methods for protecting applications and data in end devices and the cloud, and provide secure methods for data resiliency and recovery. These standards for data resiliency and recovery should be equal to or exceed the security provided the encryption and key management processes for the basic protection of the applications and data. Implementation of these standards by the technology providers and ISPs should be driven by market demand, and not by policy or legislation.

4. The President should include in future budget submissions to the Congress, sufficient resources for the FBI and the US intelligence agencies to develop new investigative and technical capabilities for execution of their missions in the face of ever evolving technologies and applications.

Protecting Privacy in the Conduct of Cybersecurity Programs

Dan Chenok

Margie Gilbert

Jayne Holland

Frank Reeder

Introduction

Protecting the nation's cyber assets also entails safeguarding sensitive personal information. Individuals frequently share facts about themselves over open networks that they would not want to be released in public, much less threatened by a malicious actor – examples include a consumer who provides financial information to enable an online bank transaction, a patient who exchanges medical information with a health care provider to pay a bill electronically, or a citizen who logs in to a government website to apply for or receive a benefit.

Given the complex array of vulnerabilities and threats that exist in cyberspace, enterprises that provide these and other kinds of information and services must continually monitor traffic on their networks to protect against constant attempts to penetrate systems for malicious, criminal, espionage, or other purposes. The teams of experts who track traffic must also take care to safeguard the privacy of individuals whose information is accessible during the conduct of legitimate cyber activity.

At the same time, the cybersecurity industry is growing more sophisticated in tools and services that government and commercial enterprises leverage to protect networks. Traditional monitoring and perimeter defense approaches are being supplemented by advanced signature analysis, analytics that can detect algorithmic anomalies that may associated with malware, and new approaches to multifactor authentication using biometrics. These and similar efforts raise new issues with regard to protecting personal information while capitalizing on advances in cybersecurity.

Because cyber protection is rising as a paramount issue for the economy and government, the Administration should work with the private sector to develop a set of principles for protection of privacy while engaging in cybersecurity activities. In addition, the Administration could develop and disseminate technical, managerial, and operational actions for practical implementation. The Commission recommends that the next Administration focus on three different policy areas in achieving this goal:

- Protecting privacy in performing government surveillance and implementing new technology over commercial networks
- Updating the Privacy Act and related law and policy to account for new technologies and bring protections into the 21st century
- Endorsing national law and policy to address data breaches and enhance cybersecurity and privacy

Protect privacy in performing government surveillance and implementing new technology over commercial networks.

In order to build confidence that protection of cyberspace respects the need to maintain confidentiality of personal information, major government and private sector actors could agree on a set of effective practices to adopt – following a model similar to the NIST Cybersecurity Framework. As with that NIST effort, government could work with the private sector to develop a set of principles for safeguarding personally identifiable information (PII) in the conduct of cybersecurity programs that incorporates robust privacy policies, such as those that implement the Fair Information Practice Principles (FIPPs) set into policy by DHS, as well as related technical, managerial, and operational actions, for protection of privacy. Such principles and

actions might include[16]:

- **Data Minimization**. Develop and implement clear data minimization rules and policies in a cybersecurity program to ensure that, consistent with the FIPPs, PII is only collected, used, or shared when necessary for program purposes, and is only collected as a necessary part of the cyber threat information.
- **Education**. Provide education, information, and tools as appropriate to government and industry stakeholders to assist with the identification and removal of PII.
- **Data Retention**. Records should not be kept any longer than needed to fulfill the purpose of the program; specifically, data retention periods for PII should be limited to the timeframe necessary to address the particular cyber threat for which the information is being retained.
- **Data Integrity**. Assure that any data under a cyber program is handled carefully to preserve its physical and logical integrity.

In addition, practical measures can be implemented by public and private organizations to build privacy protections into the conduct of cybersecurity programs. These include:

- **Adopting advanced signature analysis and analytics that can detect anomalies that may associated with malware**. Often referred to as "behavioral" or "algorithmic" analytics, these techniques enable organizations to better focus cyber resources on potential threat vectors without the need for a predetermined signature associated with an IP address.
- **Promoting multi factor authentication using biometrics**. Building on policy introduced across multiple Administrations, this approach significantly reduces the risk that PII is accessed by individuals who do not have rights to that access (whether a citizen or consumer conducting an online transaction, or a system administrator reviewing enterprise networks).
- **Assessing the need for special rules regarding mobile devices and other technologies where physical and cyber assets create "mingling" of digital data**. The vast amount of personal information on smartphones and other types of mobile devices makes it incumbent on providers and users of these technologies to adopt protective approaches that limit PII exposure if a device is lost. At the same time, the government should continue collaborating with the private sector on ways to enable appropriate access to such devices for legitimate law enforcement purposes in the face of a demonstrable threat.

Update the Privacy Act and related law and policy to account for new technologies and bring government protections into the 21st century

The Privacy Act of 1974 remains the foundational US Government privacy statute. Yet the Privacy Act was enacted in a very different information technology context, where paper or simple electronic "flat" files were the norm, and there was limited ability to aggregate information on individuals. The statute contains enduring fair information principles, but also anachronistic requirements that create unnecessary process with little privacy return, and it does not cover protecting information that is not retrieved by name in a government database. The law does not protect privacy so much as provide a process for notice, access, and redress of people to

[16] Based on the 2012 Report of the DHS DPIAC on Privacy and Cybersecurity Pilots (https://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/dpiac_cybersecurity_recommendations_11072012.pdf)

the information their government holds about them.

Revelations over the past decade have focused public attention on government's ability to use – and misuse – PII and have contributed to growing distrust of government generally. This was magnified by the two major breaches in 2015 of over 20 million records about federal employees and contractors with security clearances held by the Office of Personnel Management.

In a real-time information sharing world, where immediate and automated sharing can make a significant difference in cyber protection, the US Government needs a statute that allows for such rapid action while still protecting privacy. One model for such an update to the Privacy Act was introduced by Senator Daniel Akaka in 2012, based on a draft developed by the Center for Democracy and Technology; that bill could be revisited as the basis for a new Privacy Act that accounts for new technologies and brings protections into the 21st century. Key elements of a Privacy Act update could include:

- **Refine scope beyond system of records.** The Privacy Act's core coverage is based on the government holding information about individuals in a system where records are retrieved by a name or other identifier. But the power of analytics enables widespread and complex linking of attributes that, taken together, can identify a person in a split second, and use that information without statutory protection because it is not retained in a system. The advent of Privacy Impact Assessments over the last decade has led agencies to understand the implications of such new technologies, and providing legal protections to individuals based on the much broader scope created by PII would both strengthen PII in those systems and increase public confidence that government is handling information appropriately in the conduct of cybersecurity programs.
- **Revise and simply notice.** Millions of Americans receive privacy notices every day; they are often contained as boilerplate language in federal forms that serve as models for other levels of government and even commercial activity. But the bureaucratic and legalistic language of these notices, combined with their general applicability that often has little relationship to the actual transaction involving an individual, has led most Americans to simply ignore their content. The Privacy Act could be revised to call for meaningful, clear notice that is connected to a governmental purpose for collecting PII, and to require that agencies leverage technology to tailor notices according to the sensitivity of the transaction. For example, a notice for reserving a campsite would differ from one for filing taxes.
- **Adopt a risk-based standard for privacy response, similar to risk management approach to security under FISMA.** The FISMA statute referred to elsewhere in this report is based on a decades-old premise, which states agencies should develop risk-based security measures – developing security approaches that balance the risk and potential magnitude of harm from an incident against the benefit created by the system. The Privacy Act, and privacy law generally, is premised more on a legal standard of coverage and compliance – once coverage is determined (see above), there are a set of mandatory procedural actions that agencies must take, rather than a decision process for the agency to follow in determining an appropriate protective level. In a world where billions of bytes of data fly across federal networks every day, agencies could focus their limited resources on real threats to privacy by adopting a risk-based standard under a revised Privacy Act.
- **Endorse national law and policy to address data breaches and enhance cybersecurity and privacy.** Currently, notification requirements in the event of a security breach involving

PII are dictated by state law with 47 states, as well as the District of Columbia, having enacted data breach notification laws. While there are some similarities amongst the state laws, the differences among them are not insignificant. There is no comprehensive federal approach or legislation that addresses this issue; many companies are therefore required to comply with a patchwork of laws that exist in the states where the impacted consumers are domiciled. This can be challenging, frustrating and confusing; to better protect data and become more expeditious and transparent in reporting security breaches from a practical standpoint, one standard may make sense.

A national data breach notification statute would bring uniformity in how impacted consumers and other key entities are notified when consumer's PII has been compromised. Such legislation, which has been introduced in multiple legislative proposals, could preempt similar state breach notification laws, including a common definition of PII.

A national data breach law could include a number of elements that promote privacy and enhance cybersecurity:

- **National PII definition.** Introduce a national approach to definition of PII, breach notification, and response, premised on good commercial practice plus federal regulatory framework through agencies like FTC and FCC.
- **Amend the Fair Credit Reporting Act**. Require credit reporting agencies to notify individuals whenever their accounts are pinged, so that they can act quickly if accounts have been compromised through a breach.
- **Align national law with international norms.** In a world where cross-border data flows carry personal information into multiple jurisdictions, often in the conduct of a single transaction that is conducted over global and "cloud-based" networks.

Finally, the next Administration could develop policy to reduce risk posed to personal identifiable information (PII) when collected by commercial data aggregation. Commercial data aggregators and big data brokers—companies that collect consumers' personal information and resell or share that information with others—participate in the economy based in part on the premise that citizens lack the right to deny resale of their personal information for profit. Massive stores of big data in the possession of third party data brokers constitute a wealth of information for malicious actors to capitalize through a few large data breaches. Neither government nor industry has been spared from these exposures, as seen over the past few years; the long-term effects on individual or company assets have yet to be evaluated. There may be a "tipping point" that leads to government intervention as private entities get overwhelmed with continued exploitation of their data holdings. While not a government regulated "sector," the next Administration should consider risks posed to PII when collected by commercial data aggregation companies.

Establishing the U.S. Consumer Cybersecurity Product Safety Commission (CCPSC)

Introduction

Dependence on the Internet has never been higher, nor have the dangers to individuals and public and private enterprises. The spectrum of consumer harms that could result from poorly designed or manufactured cybersecurity products and services is growing in volume and severity.

This paper describes elements of the current environment, identifies some key technology challenges, highlights current federal government organizational responsibilities and gaps, and focuses on options to address one important aspect of the challenge—government's role in improving consumer cybersecurity products and services. Establishing the U.S. Consumer Cybersecurity Product Safety Commission (CCPSC) would allow the government to improve cybersecurity products and services, identify insecurities, respond to infractions, educate consumers, and improve coordination with the private sector.

The Current Environment

Reliance and Threats

Dependence on the Internet has never been higher, nor have the dangers to individuals and public and private enterprises. The US population with Internet access skyrocketed from about 10 percent in 1995 to about 80 percent in 2014. E-commerce as a percentage of total retail sales was less than one percent in 1998 and grew to nine percent by 2014. More Americans are relying on the Internet for the basic necessities of life, including using on-line services to acquire food, clothing, shelter, and work. Government communications and functions also rely on the Internet. The Obama Administration's, Digital Government Strategy, states "...New expectations require the Federal Government to be ready to deliver and receive digital information and services anytime, anywhere and on any device. It must do so safely, securely, and with fewer resources. To build for the future, the federal government needs a Digital Strategy that embraces the opportunity to innovate, do more with less, and enables entrepreneurs to better leverage government data to improve the quality of services to the American people." Each federal department and agency also relies on the Internet to perform its mission — including classified national security work. Although not owned and operated by the government, the Internet and related telecommunications infrastructure also provide the backbone upon which other critical infrastructures, like transportation, oil and gas pipelines, and the finance and banking industries, are dependent.

As our national dependence on the Internet has grown, so too have cyberattacks and cybercrimes that threaten US interests. For the first time in history, the US Director of National Intelligence ranked cybercrime as the top national security threat, higher than that of terrorist attacks, espionage, and weapons of mass destruction. As an example of the Internet being used as a vehicle to commit crime, FBI Director James Comey reiterated his concerns about the FBI "going dark" and that the terrorist group ISIS is using encrypted communications to actively recruit jihadists in the United States. Ben Wittes, Editor-in-Chief, Lawfare, is troubled by the extent to which the ISIS concerns and the going dark concerns have converged, noting "There are people in the United States whom authorities responsibly believe to be in contact with ISIS for whom surveillance is lawful and appropriate but for whom useful signals interception is not technically feasible."

The private sector cannot provide adequate defenses against these attacks as businesses are incurring increasingly frequent and costly cyberattacks. Most organizations' cybersecurity programs do not rival the persistence, tactical skills, and technology prowess of today's cyber adversaries, and arguably the asymmetry will persist for the foreseeable future. A related survey found that seven percent of U.S. organizations lost $1 million or more due to cybercrime incidents in 2013 compared with three percent of global organizations. Based on a Federal Trade Commission Report, consumer fraud and identify theft complaints rose from about 2.2 million in 2013 to about 2.6 million in 2014 — an 18 percent increase. General public awareness about these threats is also on the rise thanks to popular media coverage about events like the hack on Sony Entertainment computer systems, Target, and Home Depot and data breaches of personal information experienced by major health care insurers. The exfiltration of an estimated 22 million personal records of government employees from an Office of Personnel Management database is another recent example.

Potential Harms

The spectrum of consumer harms that could result from poor cybersecurity products and services is growing in volume and severity. For individuals, financial loss resulting from identity theft causes significant damage. Other activity, including cyberstalking and cyberbullying, may lead to physical and emotional harm to individuals. Privacy and free speech concerns are mounting and are well documented. As the Internet of Things (IOT) matures, grave physical consequences, even death may occur through Internet abuse. Imagine scenarios where medical devices, like pacemakers or medicine delivery systems, are controlled via the Internet. If data and infrastructure are not appropriately secured, then loss of life is possible, as exemplified in the recent "car-hacking research" that allowed two attackers to gain remote control of the vehicle via the Internet and sent a vehicle into a ditch in St Louis, Missouri. Lights, heating and cooling, and security systems for homes are already controlled using mobile phones and related data resides on the Internet. A criminal with cyber savvy could by-pass alarm systems, identify specific houses, and easily break and enter to rob unsuspecting owners.

For industry, vulnerable information systems, networks, and computers may result in loss of public trust and undermine confidence and potential growth in electronic commerce. Data, intellectual property, and trade secret theft reduces economic competitiveness and has a negative impact on brand integrity and products. Growing harms to all users is one reason why improving the quality of consumer cybersecurity products and services should be considered.

Role of Government

Gaps exist between public perceptions, expectations, and bona fide federal responsibilities and accountability for cybersecurity. Recent significant data breaches, foreign cyberattacks against U.S. commercial entities, and upticks in cybercrime have many calling for government action. In a 2014 Dell software survey, nearly 80 percent of U.S. IT industry leaders believed the federal government plays a key and positive role in protecting enterprises from international and external cyber threats. Close to 90 percent of all respondents worldwide said government should help determine security defense strategies of organizations.

Popular consensus that government has a role to play in cybersecurity does not extend to a clear scope of government action or the specifics of the government role. Some think the

government should focus on frameworks and not mandates. Additional themes in the press indicate that the U.S. government should have the responsibility to find and then release all vulnerabilities to help improve the state of cyber security. Others advocate a far more limited role for government.

In reality and despite public perceptions, government's role in protecting the Internet is limited and mostly focused on government's classified and unclassified computer systems. No single entity in the federal government has responsibility devoted to the security of commercial and consumer information systems.

Adding to the debate and contributing to confusion are pronouncements in recent National Security, Department of Defense Cyber, and Intelligence Community Strategies that call for increased public/private partnerships to secure this domain. The 2015 National Security Strategy specifically states, the United States will "take necessary actions to protect our businesses and defend our networks against cyber theft of trade secrets for commercial gain whether by private actors or the Chinese government." Some press reported that this sentence is noteworthy, because it clearly states for the first time that the U.S. government takes responsibility to protect the private sector from cyber-espionage. The President's Review Group on Intelligence and Communications Technology concluded that strong cybersecurity and strong encryption should be vital national priorities and recommended, among other things, that the US Government should fully support and not undermine efforts to create encryptions standards...increase the use of encryption and urge US companies to do so.

As a practical matter federal agencies, although not specifically chartered, are posting consumer related helpful hints and tips as a way to help improve cybersecurity. In 2011, former Senate Select Committee on Intelligence General Counsel, Daniel Gallington wrote about unique U.S. risks to protecting these assets, "Our tradition of private enterprise and limited government could make us more vulnerable to cyber threats. It also limits the federal government's ability to influence key security aspects of our cyber and other critical infrastructure."

Technology Challenges

Challenges in today's information technology are similar to other times in history when transformative and disruptive technologies required changes in landscape, uses, and protections. For example, acceptance and widespread use of automobiles and aircraft resulted in the need for new roads, new infrastructure, and new rules and regulations for safety and security. What is different now/today/etc. is the speed and complexity with which changes to the IT domain are occurring. Acceptance and growth of automotive- and aircraft-related safety industries took many decades to mature and implement, as did associated governmental regulatory regimes. Widespread dependence on the Internet occurred much more rapidly. Today, Internet technology, products, and services advance in months not years. The Internet itself morphs at the blink of an eye.

Protecting the Internet is not a monolithic endeavor. It's not just computers or devices that require protection. Data, networks, hardware, software, physical and virtual infrastructure, and storage are some of the multi-faceted and interconnected elements that require security. Vulnerabilities are everywhere and they are temporal, and shoring up protections in one area

may open holes in other areas. Additionally, users have different needs and adopt security solutions at different rates.

The complexity of the Internet is rivaled only by the complexity of the security products and services necessary to protect it. Even experts don't agree. According to Daniel Geer, In-Q-Tel Chief Information Security Officer, if perimeter control is to remain a paradigm of cybersecurity, then the number of perimeters to defend in the Internet of Things is doubling every 17 months. Others believe that computer hygiene is the best way to improve computer and network security. Different experts think strong encryption is critical. Eric Schmidt told a 2014 Stanford University gathering, that the key to cybersecurity is cryptography. While encryption may be a poster child for cybersecurity, it is by no means the only security element required for a free and open Internet. However, it's a useful surrogate term and offers some insight in the complexity of both cybersecurity technology and its use. "Cryptographic software we have today hobbles those who try to use it with Rube Goldberg-machine complexity and academic language as dated as a pair of Jordache jeans...Nobody really wants cryptography in and of itself. What they want is to communicate how, and with whom they please, but safely." In most cases security features are kludgy add-ons to existing systems and user experience continues to be lacking.

In the past, cryptography was the near exclusive domain of governments. Encryption used for both code-making and code-breaking was created to protect national security information and to exploit vulnerabilities of foreign adversary's communications. However, this paradigm has changed with increased demand for consumer-related products and services to promote commerce and enable security, privacy, and confidentiality. According to one study, "Despite large investments [by the private sector] in security technologies, lack of skilled experts continues to result in breaches." At least 30 percent of organizations cite a problematic shortage of each of the following: 1) cloud computing and server virtualization security skills; 2) endpoint security skills; 3) network security skills; 4) data security skills; and 5) security analytics/forensic skills." Even as this expertise matures, *who is responsible for making sure the commercial security products and services work as advertised?*

Perhaps one of the most telling indicators comes from the growth in cybersecurity products and services. Consumer cybersecurity products may be considered those tools, hardware, software, devices or techniques that are not solely built or mandated for use in U.S. Government systems, but are generally available for purchase by the public. "The need for what we have heretofore called cybersecurity is now so varied that it is no longer a single field but many. There are over 800, perhaps over 1000 cybersecurity startups in some stage of the funding game...Cybersecurity is perhaps the most difficult intellectual profession on the planet" noted, Greer.

Neither Internet technology, nor related security measures, nor assessing harms from cyberattacks and cybercrimes are easily understood or managed. Although there is increased public discussion in these areas, much work remains. In sum: *now that we need cybersecurity protections to the degree that we do, to whom does the responsibility devolve?*

Federal Government Responsibilities

A key underlying factor in future discussions of federal government responsibilities is that the once distinct lines between and among national security systems, other government systems, critical infrastructure, commercial, and personal data are blurring. Two significant consequences follow from this observation:

- Translating US governmental responsibilities from actions in the physical domain to the cyber domain are not always clear. For example, if a foreign adversary were to launch a missile and attack a part of the United States, then the Department of Defense (DoD) would be responsible for the military response, the Federal Bureau of Investigation (FBI) would pursue related attribution and criminal investigation, and the Department of Homeland Security (DHS) would help local officials with emergency response and recovery. In cyberspace, if a "logic bomb" was lobbed against a business, but resulted in damages to an entire region or sector, and because attribution and intention are difficult challenges, it's not clear whom or how a response would be carried out. Perhaps the cyber roles and functions should follow the physical ones, but there is no significant legal precedent to follow.
- A weak link in one system could lead to consequences and failures in others. One of those links may be commercial security products and services used by consumers.

Today, no single federal entity is responsible for the quality and efficacy of consumer cybersecurity products and services. Before turning to *how* government could be postured for improving cybersecurity in products and services used by the private sector, it's worthwhile noting existing federal responsibilities for cybersecurity.

Within the White House, OMB Memo 10-28 outlines and clarifies the respective roles of OMB, the Cybersecurity Coordinator and DHS. For OMB, it states OMB is responsible for the annual FISMA report to Congress, the development and approval of cybersecurity portions of the President's Budget, the traditional OMB fiscal oversight of USG's use of funds and for coordination with the Cybersecurity Coordinator on policy issues related these responsibilities.

"The complex federal role in cybersecurity involves both securing federal systems and, in some cases, assisting in protecting non-federal systems. Under current law, all federal agencies have cybersecurity responsibilities related to their own systems, and many have sector-specific responsibilities for critical infrastructure. More than 50 statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place."

"In addition to the roles of White House entities, the Department of Homeland Security is the primary civil sector cybersecurity agency. The National Institute of Standards and Technology (NIST), in the Department of Commerce, develops cybersecurity standards and guidelines that are promulgated by the Office of Management and Budget. The Department of Justice is largely responsible for the enforcement of laws related to cybersecurity." The Federal Bureau of Investigation (FBI) lists among its priorities the protection of the United States from 'foreign intelligence operations and espionage' and `cyber-based attacks and high-technology crimes.' FBI is often involved in investigating computer network attacks. The National Science Foundation (NSF), NIST, and DHS all perform research and development (R&D) related to cybersecurity. The National Security Agency (NSA) has a focused role as the information

assurance agency for National Security Systems (NSS), although other agencies play significant roles due to the interdependence of systems, services, and products. U.S. Cyber Command, part of the U.S. Strategic Command in the Department of Defense (DoD), has primary responsibility for cyberspace operations."

Government National Security Systems (NSS)

NSS are information systems operated by the U.S. Government, its contractors, or agents that contain classified information or systems that involve intelligence activities, cryptographic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system(s), or systems critical to the direct fulfillment of military or intelligence missions (not included are routine administrative and business applications) Leighton Johnson, "Security Controls, Evaluation, Testing, and Assessment Handbook,".

Most responsibilities for protecting NSS fall to the Secretary of Defense as the executive agent for NSS and more broadly to Defense Department components. NSA is specifically directed by National Security Directive 42 and DoD Directive 5100.20 to take responsibility for prescribing minimum standards for protecting cryptographic and sensitive techniques and information to be employed by National Security Systems (NSS), and for ensuring that public security standards address national security systems protection requirements. Within NSA, its Information Assurance Directorate (IAD) has the mission to protect and defend National Security Information and Information Systems. But even NSA often relies on commercial security products and services to protect these systems and DoD relies on the commercial Internet and the public networks for its own communications.

To make sure security products are safe for government classified systems, NSA sponsors a variety of programs to address cybersecurity in areas outside of the formal NSS domain. The NSA initiative, Commercial Solutions for Classified (CSfC), relies on layering commercial security products to protect National Security Systems. NSA also sponsors the National Security Cyber Assistance Program (NSCAP), which "accredits qualified organizations to perform select cybersecurity services in support of [NSS] owners and operators. Another effort is the National Information Assurance Partnership (NIAP). NIAP is responsible for U.S. implementation of the Common Criteria Evaluation and Validation Scheme (CCEVS). Members of the Scheme agree to a unified approach to evaluating information technology products and protection profiles for information assurance and security. Commercial companies wishing to sell to their cybersecurity products for use in NSS, must comply with the protection profiles and have their equipment evaluated.

Government Non-NSS

For non-NSS operated by the U.S. Government, its contractors, or agents, (e.g., Office of Personnel Management (OPM), Internal Revenue Service (IRS), and unclassified State Department computer networks), DHS states that it "has the lead for the federal government for securing civilian government computer systems."

NIST is responsible for establishing and promulgating security standards and guidance for these systems. While the standards apply to government networks, NIST also makes the standards available to the public. NIST publishes Federal Information Processing Standards

(FIPS) for many security products and specifically controls the FIPS Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) evaluation processes. NIST is also responsible for certifying commercial testing laboratories that conduct Common Criteria evaluations through the CCEVS and the FIPS140-2 testing labs. The National Voluntary Laboratory Accreditation Program (NVLAP) is an evaluation conducted by NIST to ensure FIPS and Common Criteria labs are up-to-date and consistent with their physical, policy, and quality assurance measures.

Privately Owned Critical Infrastructure

Federal government responsibilities for protecting commercial and private systems have been focused mostly on private sector elements that own and operate what are considered critical infrastructure and key resources, as well as developing new methods and tools for sharing threat information with critical infrastructure owners. DHS considers critical infrastructure to be any assets or systems that are so vital to the country that if damaged or destroyed, there would be a debilitating effect on the U.S. public health, safety or economic security. DHS is the only federal entity that has some responsibility for protecting these networks in the context of working with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. DHS also operates the United States Computer Emergency Readiness Team (US CERT) which "leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans". The Federal Communications Commission has a division for "Cybersecurity and Communications Reliability," which focuses on ensuring reliability, redundancy, and security of US communications infrastructure.

Business and Consumer Information Systems

The final category of information systems, networks, and computers are those owned and operated solely by private companies and individual citizens. Based on a cursory review of federal agencies' responsibilities there are few government organizations dedicated to providing cybersecurity support to the general public. The Federal Trade Commission (FTC) has investigative and enforcement authorities that cover unfair or deceptive data security practices. Other federal agencies, (e.g., Federal Communications Commission (FCC) and Federal Aviation Administration,) also have limited authorities and remedies available to influence and manage cybersecurity measures taken by industry sectors under their purview.

Responsibilities of Non-Government Entities

Standards Bodies

In addition to government-only entities, voluntary standards development organizations and industry consortia exist for a variety of Internet and related communications technologies. Many of the U.S. based standards organizations and industrial consortia are private sector organizations. These organizations are vital to the operation and security of the Internet and communications. This is one reason why official U.S. policy directs "agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with

law or otherwise impractical," and encourages standards that will meet public and private sector needs.

For cybersecurity, standards include: cryptographic techniques, cyber incident management, identity management, network security, security automation and continuous monitoring, supply chain risk management and software assurance. Standards development organizations usually have one or more subgroups concerned with cybersecurity core areas. For example, the Internet Engineering Task Force (IETF) is comprised of approximately 100 working groups. Each working group sets technical standards for the Internet including areas such as network security, identity management, cyber incident management and security automation and continuous monitoring.

The United States Standards Strategy, developed by stakeholders in industry, government, standards developing organizations, consortia, consumer groups and academia, emphasizes a "market-driven, private sector-led approach to global standardization." The strategy also recognizes that the U.S. national interest in emerging areas of standardization, such as cybersecurity will require "public and private sectors, standards development organizations (SDOs), and consortia find new ways to work together in order to preserve national competitiveness."

The American National Standards Institute (ANSI) founded in 1918, is a leading U.S. organization in this area and has a critical role in coordinating and promoting voluntary consensus standards and conformity assessment systems. ANSI is the U.S. representative in non-treaty, international and regional standards-setting activities.

Non-profits/Open Source Initiatives

Many non-profit and open source initiatives already exist. For example, the SANS Institute was established in 1989 as a cooperative research and education organization and provides information security training and security certification. As part of their work, SANS formed a set of recommendations known as the 20 Critical Security Controls. In 2013, the stewardship of these controls was transferred to the Council on Cyber Security, another independent, global non-profit organization. The Electronic Frontier Foundation publishes information about cybersecurity vulnerabilities and practices, including comments on existing and future laws and policies.

Looking ahead, former Google computer security researcher, Peiter Zatko, tweeted in June 2015 that he is leaving his current position to stand up an "Underwriters Laboratories (UL)-type organization for security standards testing and certification for the Internet of Things. This was later followed with a contract from the Air Force (on behalf of DARPA) in September. DARPA spokesperson Jared Adams advised the Cyber Independent Testing Laboratory is proposed in two tracks that run in parallel: “The first track defines the metrics, ratings and certifications required to provide actionable measurements of software risk. The second track describes the mechanisms and processes needed to assess existing software according to the metrics defined in the first track.”

US Consumer Cybersecurity Product Safety Commission

Parallels to the Consumer Product Safety Commission

If the state of play in the current governmental, consumer, and public interest milieu has a familiar ring, it's because these factors bear similarities to another time in recent history — the rise of consumer advocacy and the creation of the Consumer Product Safety Commission (CPSC). Until the early 1970's, the federal government relied on a mixture of laws and agencies to protect consumers from faulty products. No single agency was responsible for enforcing these laws. No agency had jurisdiction to regulate the sale and manufacture of certain products that were not already covered by another federal entity. Consumer education was sorely needed. No single government entity offered avenues for consumers to report concerns about unsafe products or injuries. Harms as a result of faulty products (from flammable fabrics, to cribs, to vehicles) were growing, as was increased public attention. For all these reasons, Congress passed and the President enacted the United States Consumer Product Safety Act in 1972, which included establishing the CPSC.

As an independent regulatory agency, CPSC's mission is "protecting the public against unreasonable risks of injury from consumer products through education, safety standards activities, regulation and enforcement." Many of CPSC's core activities also align with current consumer needs in cybersecurity, including facilitating development of effective voluntary standards with a broad range of stakeholders, issuing and enforcing mandatory standards, initiating recall or corrective action, conducting research on potential consumer product hazards, informing and educating consumers, and encouraging industry to implement globally recognized best practices.

Establishing the U.S. Consumer Cybersecurity Product Safety Commission (CCPSC)

Creating a new federal entity or adding missions to an existing federal agency is fraught with challenges, not the least of which are increased financial costs to taxpayers, wresting mission and authorities from existing entities, and responding to industries' position that regulation hampers commerce. Nevertheless, a U.S. Consumer Cybersecurity Product Safety Commission (CCPSC) may address a gap in responsibilities of this growing market. As a "one-stop shop" for consumers, this organization can help simplify and navigate complex technical challenges, offer a place for consumers to lodge complaints, and act as a liaison with other related public and private entities. Additionally, raising the bar for consumer cybersecurity could help reduce vulnerabilities in other sectors as well as increase user-friendly cybersecurity market demand.

Based on the primary functions of CSPC, the CCPSC would help protect American consumers through five primary activities:

1. **Improve:** Improving cybersecurity products and services through regulatory actions and monitoring and contributing to voluntary standards creation would help prevent insecure cybersecurity products including cryptography from reaching consumers.
2. **Identify:** Identifying cyber insecurities may include gathering and analyzing information from tip lines, self-reporting from industry, and testing and evaluating products and services. Issuing public reports based on results would be a core function.

3. **Respond:** Responding to identified product insecurities could include regulatory and enforcement activities to compel producers to correct known problems. The Commission would also need mechanisms to address problems identified in open source cryptography/cryptographic implementations.
4. **Educate:** Consumer education would be a large component the organization. Education could focus on both consumers and industry. Communications vehicles could include public service announcements and information on a CCPSC web site that list and explain existing risks, identify recalled products, and offer standardized remediation advice. For the cybersecurity product and services industry, the same vehicles could be used to announce changes to regulations or standards and promote information sharing.
5. **Coordinate:** To make best use of processes and expertise that already exist, CCPSC could be a conduit for sharing with the public many of the standards, best practices, and lists of products that the government uses, including some that are used to protect classified information. This would offer a one-stop-shop for consumers. Within the U.S. Government, the CCPSC could participate and bring the consumers' perspective to existing entities for standards monitoring, vulnerabilities processes, evaluation and certification regimes, and export controls.

Success will depend upon recruiting, retaining, and developing a highly skilled work force with diverse talents and expertise. Among the necessary core skills are: expertise in cybersecurity, cryptography, regulation writing, investigating problems with cybersecurity products, creating compliance programs, consumer outreach and enforcement, and achieving buy-in and cooperation from Congress, other parts of the federal government, industry and the general public.

Conclusion

Addressing Internet safety and security requires us to think differently about the roles of government, industry, and consumers. We must consider new and rapidly changing challenges in a world of a shared commons -a space that is simultaneously owned by everyone and no one with a technology that advances so quickly that no one entity can keep pace. Improving consumer cybersecurity products and services and ensuring they work as advertised is one of many challenges that requires the creativity, know-how, and technical expertise of those in government, industry, and the international community working together to achieve solutions. A U.S. Consumer Cybersecurity Product Safety Commission offers one model for consideration and provides a more tangible point for discussion and analysis of the complex web that is cyberspace and the complex set of entities and functions that are designed to improve cybersecurity.

Dealing with Restricted Global Flows of Data

Stephen Lilley

Paul Rosenzweig

Introduction

Cybersecurity has become a tool by used by nations to restrict free speech, global flows of data and to more broadly restrict global trade. It is in the United States' interest to advocate for the liberal flow of data around the globe and ensure that its bilateral and multilateral agreements continue to include and create global norms that allow for free-flowing movement of data and cybersecurity rules of engagement.

Recommendations:

- The next President should develop a strategy for an economic and diplomatic offensive to maintain and expand free flows of data around the globe and ensure a seamless approach to cybersecurity.
- Components of that strategy should include efforts to:
    - Underscore existing agreements within the G7 and G20 that cybersecurity will not be used for economic espionage;
    - Reach agreement with like-minded countries on baseline standards of privacy and civil liberties;
    - Reach agreement on choice-of-law rules that would apply in the absence of agreement on baseline standards;
    - Adopt a declaratory policy forgoing unilateral extraterritorial data demands conditioned on:
        - Reciprocal forbearance other nations; and
        - A commitment of the requisite resources to be responsive to MLAT requests;
    - Expansion of the existing US-UK negotiations and mutual recognition of legal process to other nations; and
    - Internal MLAT reform, speeding cooperative data flows that are not subject to the mutual recognition process.
    - Continue to negotiate against restrictive data localization requirements by other nations

Summary of the Problem

The global nature of trade and services, along with the exponential nature of the connectivity of services around the world brings increasing conflict between sovereign nations. The growth in cross-border trade in services is rendering traditional choice-of-law rules problematic at best. It also means there is a growing need for modifying now quickly outdated diverse legal systems to provide protections to global corporations and the United States.

Geopolitical strife and the increasing boldness of authoritarian nations has resulted in in nation states and non-state actors who use cybersecurity as a tool against the US and our companies. These efforts fit under the general rubric of the growing implementation of data localization requirements by China, Russia and other nations around the world which is contrary to what global trade should really be about.

Discussion

We believe that cross-border trade in services and free-flowing data are part of a global economy that should be encouraged, not stifled. The following lays out a strategy for achieving that goal and can form a blueprint for action in the next Administration.

We begin with a simple premise: global data flow restrictions are, in effect, a non-tariff trade barrier and protectionist measures. We are seeing increased examples of this phenomenon that range from data localization requirements, to restrictions in in-bound flows of data, to limitations on the exchange of data (often, though not always, grounded in privacy concerns). These limitations are embodied in cybersecurity issues, technology protections, privacy rules and law enforcement access restrictions.

Each of these shares a singular characteristic – unilateralism. That is the assertion by a nation that its laws control actions by evidence holders, irrespective of other countervailing interests. Increasingly, nations are putting mandates on citizens and global corporations for protectionist measures and/or as a means to use it as a global tool, and in some cases, weapons against companies. China, for example, has mandated that citizens register for access to the network and that providers maintain encryption back doors in products to enable access as a condition of being permitted to sell in Chinese markets. Other nations are increasingly taking similar actions. As the US continues to negotiate agreements, it is critical that those actions that clearly conflict with existing legal obligations be immediately called out.

Data localization is one example where nation states are increasingly institutionalizing restrictions on global corporations both as a means to expand their own economic security but for national security and global espionage. Cybersecurity and privacy issues are increasingly on the forefront of the global policy agenda and but managed in a bifurcated manner. The recent renegotiation by the US and the EU over what was Safe Harbor and is now Privacy Shield is a useful example. The EU has drawn a line in the sand on cybersecurity and privacy issues, and the implementation of the new General Data Protection Regulation (GDPR) and the Networked and Information Security Directive (NIS) are examples of the new patchwork nature of these news laws, along with other countries like Russia, China, Brazil, India and many others. Privacy concerns in a post-Snowden world are driving many nations to say that decision making is in the hands of individuals. At the same time, there must be a balance for how global trade can and should continue.

Effects

There are several consequences of this trend. The first is economic – data flow restrictions distort global economics forcing companies to manage a complex and fragmented system and potentially putting the US at risk if nation states require “back-doors” to US companies’ systems. The most obvious cost of the current system is the sheer complexity and the costs of compliance. Thus, continued unilateralism and the growth of data localization are forecast to cause noticeable GDP, investment, and welfare losses.

The compliance costs are, however, just the tip of the iceberg for transnational companies. As an example, the current rules for law enforcement access to cloud-based evidence are affecting the perception of consumers and thus causing injury to their brands.

The second area of effects is social and political. Some nations see data flow restrictions as a way of suppressing dissent and strengthening their own domestic controls. Others see restrictions as ways of protecting domestic industries and projecting domestic cultural norms. As a general matter, the United States has a broad interest in democratizing norms of behavior and allowing the free flow of ideas. Data flow restrictions work against those basic goals.

Finally, the trend towards data flow restrictions will have inevitable effects on law enforcement and national security concerns, for the United States and for other nations. Law enforcement agencies are finding it harder to identify and collect criminal evidence. The free flow of data obscures locations, and data is increasingly beyond the reach of lawful access.

Efforts to Date

The US government and global corporations have raised these conflict-of-law issues as a matter requiring urgent resolution. US companies are finding that they are receiving a growing number demands for data with which they are challenged to comply with due to conflicting domestic privacy laws. Law enforcement officials are increasingly finding that they that they are unable to gain access to the data they need for criminal investigations and prosecutions due to outdated legal authorities and procedures. Events such as the passage of Russia's Federal Law No. 242-FZ in 2015 and others are creating great uncertainty and violating the views of the global community about the free flow of goods and services around the world.

To date, the US government has worked to address these issues in a bilateral and, in certain instances, multilateral way with varying levels of success. Efforts to reform the Mutual Legal Assistance Treaty (MLAT) system, an outdated system that is still the primary legal means by which governments coordinate law enforcement access to data, has not been successful. It would also be important to call on Congress to complete reforms of the Electronic Communications Privacy Act (ECPA), a key law governing how US companies can provide data to law enforcement, have similarly made little headway.

US diplomats and trade negotiators have successfully negotiated strong language in support of the open Internet and the free flow of data in such venues as the Organization for Economic Cooperation and Development (OECD), the NetMundial Global Multistakeholder Meeting on Internet Governance, the U.N. World Summit on the Information Society, the Group of 7 and 20 (G7 and G20 respectively) and elsewhere, but while such language may be useful for the development of global norms surrounding data flows, these agreements and statements are legally non-binding and thus non-enforceable. Stronger and potentially binding language prohibiting arbitrary data localization rules was included into in sections of the Transpacific Partnership (TPP) trade agreement and it is critical that this agreement move forward.

Substantive Objectives

Two objectives are theoretically plausible – agreement on baseline standards of cybersecurity, privacy and civil liberties, and agreement on choice-of-law rules that would apply in the absence of agreement on baseline standards. As an initial matter we see the former as far more difficult to achieve than the latter, and recommend choice-of-law as an initial focus (along with MLAT reform) for the next Administration, with broader agreement as a more aggressive secondary goal. The task force does not express a view as to which choice of law rule might best apply.

Efforts could review and consider a variety of options, from a rule based on a jurisdictional rule that could determine the applicable law based on the locus of the harm to debating rules based on the data creator or data owner. Global trade in services and the needs of critical infrastructure companies mean that these options vary in impact, however identifying and discussing options like this are important to debate.

Procedural Methods

The next Administration should negotiate both bilateral and multilateral agreements to maintain and expand free flows of data around the globe. This strategy uses bilateral agreements to build substantial coalescence around norms that the Administration can press to be included in multinational agreements. Each agreement should prohibit data localization; commit to allowing cross-border data transfers; and describe available data transfer mechanisms.

The next Administration should expand protections for international data flows in bilateral agreements. Existing agreements with Panama and Korea recognize the importance of the free flow of information in a manner that can serve as a starting point for other bilateral agreements going forward. The next Administration should pursue these bilateral agreements where possible – and particularly with strategic partners – in order to build a critical mass of agreement that can support future multilateral negotiations. Both in creating new agreements and expanding existing agreements, the Administration should ensure that an agreement's scope is not limited by industry sector and that the agreement imposes binding and enforceable standards.

The Administration also should use regional and multinational agreements to bolster protections provided by bilateral agreements. The Administration should seek to build on the gains made in the Transpacific Trade Partnership in negotiating the U.S. – EU Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA). Both agreements should provide for the free flow of data and prohibit data localization requirements. In addition, the Administration should seek to use less formal negotiations such as the G20 and the Asia-Pacific Economic Cooperation to advance the goal of ensuring free data transfers.

Finally, the Administration should foster the development of international norms on Internet usage that will support the free transfer of data. For example, the United States and Japan have agreed to a balanced set of principles for an open Internet that will encourage the free transfer of data. Broader acceptance of equivalent principles will create a more favorable environment for the negotiation of relevant agreements going forward.

International Cybersecurity Strategy

Rich Baich

Introduction

The 2009 Report advocated a comprehensive approach to international cybersecurity using all the tools of national power. The central points included developing norms, confidence building measures, and effective deterrence.

There has been real progress in implementing these recommendations, but the world is a very different place than it was in 2009, much more conflictual and much more dependent on cyberspace. There have been important political changes as well, with the 2013 recognition that international law, the UN charter, and national sovereignty, all apply to cyberspace. The US international strategy, released in 2011, needs to be replaced to better fit a different world.

The next President will need to make key decisions on international framework for stability in cyberspace, on deterrence and response, and on law enforcement cooperation. These are the areas of greatest challenge, but the single greatest challenge may be in deciding how to engage with Russia and China, our most powerful and active opponents in cyberspace.

A Formal Approach to International Stability

The next President will need to address two major questions on the direction of international cybersecurity: is it time to consider a more formal approach to building security and stability in cyberspace, and to what extent should expanded or even continued efforts focus on agreement among likeminded states.

There has been some progress on getting agreement on norms and confidence building measures, but this approach has been largely ad hoc and may be of declining utility. It may be easiest in the first years of the next administration to continue this ad hoc approach, but before the end of the term, the US will need a new strategy for better coordination among like-minded nations, for engaging "swing states" like Brazil and India on cybersecurity issues, and a more persuasive narrative for a global audience. Setting up bilateral dialogues was a good start but it is time to move beyond this to seeking agreement.

In this, like minded nations would agree to act responsibly, practice restraint, and shape the international cybersecurity effort in ways consistent with security, stability and the protection of human rights. Any agreement would not be formally binding, but would create shared expectations for responsible behavior in cyberspace. Not having to trim and concede any agreement to win Russian and Chinese approval would allow for the development of the more robust international system we will need to secure this increasingly important domain.

The next President will need to parse proposals for agreement among those we are likely to get global support for and those that will meet opposition from authoritarian regimes. Measures focused on reducing the risk of escalation or misunderstanding will appeal to Russia and China. Measures that define responsible behavior to include support for human rights and constraints on cybercrime will be less appealing to them. The US will need a two track strategy, building norms and a framework among the likeminded nations that define individual state behavior while pursing risk reduction measures with the authoritarians.

The belief in the past was that only a global approach would work, but as the international environment fragments among contending states, this is increasingly a remnant of millennial

optimism. We did not seek the agreement of the Soviet Union in all areas during the Cold War, because we know we could not get it. The situation today is becoming the same. An increased emphasis on a like-minded approach would exclude those who do not accept freedom of speech or other human rights.

Any like-minded group must, however, avoid the fate of the Council of Europe Cybercrime Convention. This cannot be a transatlantic initiative nor can it start with only a "Western" core. Important 'fence sitters" like India, Brazil, and others must be engaged from the start. The development of a like-minded process must be inclusive from the start in shaping a consensus on responsible state behavior in cyberspace. While they share to a degree Russian and Chinese concerns over the transatlantic foundation of "universal" values, it should be possible to build a partnership with Brazil and India because of their commitment to free speech and to democratic values. Essentially, they are more like the West than they are like Russia and China, and initial talks with India are promising. Building partnerships with the new powers may require flexibility and concessions on issues like Internet governance, where Brazil, India, and others will listen to China and Russia absent a more compelling narrative.

Expanding Deterrence and Consequences

The 2009 Report called for the US to develop new strategies to deter cyberattack. There have been no cyberattacks against the US (attacks that caused physical destruction or causalities) but there has been a large number of cyber espionage and cybercrime incidents and, in the last year, several troubling efforts at political coercion. We have not succeeded in deterring these actions, but they provide useful lessons on how deterrence might be strengthened.

The most important lesson is that deterrence need not involve the use or threat to use military force. The most effective deterrent actions were the threat of sanctions or indictments. These led China to agree to end commercial espionage. In international law these would be called 'countermeasures," retaliatory actions that do not involve the use of force. In arms control parlance, the U.S. would benefit from "populating all the rungs of the deterrence ladder" with the appropriate potential responses and then communicating them to opponents.

Doing this requires defining proportional responses. For cybercrime this will mean improved prosecution and conviction rates. For espionage and coercive actions (like Sony), the US will need to make greater use of threats to impose sanctions or indict.

Our one caveat here is that even with an improved deterrent policy, including a clearer declaratory policy and a more complete range of response options, some opponents will not be deterred from some actions. This argues for more work to improve our cyber defenses, but it also raises the larger problem of relations with Russia and China. Reducing the risk of cybercrime, cyber espionage or coercive acts by these nations will need to be part of a larger bilateral strategy.

An obvious candidate for replacement is the verbose and vague declaratory policy in the 2011 strategy. Declaratory policy is a crucial part of a deterrent strategy and a lack of clarity diminishes its effectiveness in deterring threat. However, increasing clarity will require the US to develop a portfolio of appropriate and proportional response.

New Measures to Combat Cybercrime

The US position for more than a decade has been that the Budapest Convention on Cybercrime is sufficient and if only everyone would adopt it, we would all be better off. This is true, but unhelpful. In the fifteen years since it was opened for signature, fifty countries have joined. At this rate, majority of the world's nations could be members by 2040. More rapid progress is needed and the fundamental problem is that key nations refuse to sign. Russia and China refuse to sign because they are a haven for cybercrime, and China, India and Brazil refuse to sign because they were not involved in the negotiations and see the Convention as a fait accompli being forced upon them.

We do not want to abandon the benefits of the Budapest convention, but we also need to break the stalemate. We recommend two steps to do so: first, penalize in some way those countries that refuse to cooperate with law enforcement. Second, find a new negotiating vehicle that preserves the benefits of the Convention but gives Brazil, India, and perhaps China in a new negotiation that provides them with the opportunity to voice their concerns. There will be, of course, objections that any reopening will undercut the Convention, but the alternative is continued slow progress.

The next administration will be forced in this (as in other issues) to balance pragmatism and ideology. The ideology of the Internet is that it is free and open. A pragmatic approach would be to impose constraints on countries that repeatedly refuse to cooperate in cybercrime law enforcement (a minimal step could resemble the FATF "Blacklist" of non-cooperative countries). The free and open Internet is fading irrespective of US actions as nations extend their rules for online activity, but we have not identified implementable constraints on countries that fail to cooperate on cybercrime. One of the lessons of the last few years that is consequences have a powerful effect in changing malicious behavior in cyberspace (in conjunction with a revitalized effort at deterrence), and the next administration should create and make public a portfolio of punitive responses for malicious cyber action.

Military Cyber Issues

Michael Sulmeyer

Introduction

The next President will be the first to inherit a military force structure for cyberspace operations charged with three missions: defend the military's networks and systems; provide offensive cyber support to regional military commands; and defend the nation from a cyberattack of significant consequences. The President will also inherit a military, an economy, and a society that are significantly and increasingly vulnerable to cyberattack, so establishing priorities and guidelines for cyber defense and offense must be a priority. This paper addresses key questions the next President will confront on military cyberspace operations.

Threats

Over the last eight years, the scale of the militarily-relevant cyber threats has grown but the threat to US interests has not radically changed. Foreign hackers continue to probe DoD's unclassified networks; phishing activities targeting members of the DoD community have grown. Several intrusions in national security systems include the 2014 intrusion into the Joint Staff's network and a 2015 intrusion into another unclassified DoD network. There is no public information available about the effects those and other intrusions may have caused. These compromises to the confidentiality of data and systems have become more frequent in their detection and occurrence, though it is unclear their sophistication represents a leap in adversary capability.

We are seeing a morphing of the threat towards holding data integrity and availability at risk (vice confidentiality and availability). Moreover, we are seeing growing use of cyber as an instrument of national power by both Russia (Ukraine electric grid) and China (theft of personnel and medical data) which portends a growing *potential* strategic threat to US interests should those capabilities be brought to bear on the US.

At the same time of increasing frequency of cyberattacks, the complexity and scope of capability possessed by competitor nation-states – Russia, China, DPRK, and Iran – continue to grow and mature. In the case of Russia, cyber is a mainstream instrument of national power, an instrument increasingly well integrated across multiple applications of cyber power (influence, disruption, and espionage key among them) and with other national instruments of state? power.

As the cyber threat landscape evolves, the most critical threats the next President will have to address will be the potential for a major power conflict and threats to critical infrastructure. Meeting these threats necessitates a policy that takes into account mission assurance and facilitates combined operations.

Potential Major Power Conflict

In the event of a conflict with another major power, each side will have strong incentives to employ offensive cyber capabilities early against the other side's military and supporting infrastructure to impede the deployment, employment, and command and control of the opposing forces. These cyberattacks, which would not kill anyone directly, are likely to appear low risk and offer a high payoff. This has important implications for crisis management - the next administration should prepare itself to make rapid decisions about the potential employment of offensive cyber capabilities, including to reduce the other side's ability to attack US military and civilian infrastructure. In this scenario, it is worth assuming that US military systems will have at

least *some* cyber vulnerabilities, though the extent and impact of an offensive cyberattack is unclear. Assuring the resilience of critical U.S. military systems, including nuclear forces and long-range strike systems, will be critical to sustaining deterrence vital to preventing great power conflict.

Threats to Critical Infrastructure

The next President will have to consider is how military cyberspace forces might be used to defend US critical infrastructure from a significant cyberattack. At present, the National Mission Force (NMF) constitutes a high-end component of the Cyber Mission Force (CMF) structure with the mission to defend the nation from a cyberattack of significant consequence. The Department of Defense has not been specific as to what exactly a defending against a "cyberattack of significant consequence" means in practice, but Admiral Michael Rogers, the commander of US Cyber Command, has indicated in recent speeches that defending critical infrastructure is at least one likely application.

The NMF is comprised of 13 National Mission Teams, as well as some number of support teams, which constitutes a rather lean component of the overall 133 team Cyber Mission Force. As such, any mission to defend critical infrastructure will have to be narrowly tailored not just in terms of the NMF's responsibilities but to focus on the most vulnerable components of critical infrastructure. Former Assistant Secretary of Defense Eric Rosenbach noted in April 2015 testimony that the NMF would likely only be called upon to defend against the top two percent of cyber threats to the nation. Prioritizing the most critical of critical infrastructure need not be public, but it should be a first step towards guiding the NMF in its possible responsibilities.

Mission Assurance

Adversary cyber activity can undermine US mission assurance of its weapons systems and their supporting platforms, and critical infrastructure maintained by and in the private sector. Protecting .mil and related networks has been the focus of the traditional defense mission for U.S. cyber forces. However, protecting off-network systems needs to be a priority. The key concern is that through a variety of mechanisms, malware can be introduced into weapons systems even without direct connectivity to an Internet-connected system. The presence of that malware may lead commanders to question the readiness of their systems and the ability of these systems to execute core functions. A threat introduced from cyberspace can have much larger consequences on the readiness of US forces to execute non-cyber related missions, such as combat air patrols or missile defense.

Combined Operations

While US allies and partners continue to expand their capabilities to engage in cyber operations, those efforts remain largely focused on increasing resilience and defensive operations with combined offensive cyber operations remaining a distant second priority. Even then, individual nations are likely to retain tight control over their cyber capabilities and the means through which those capabilities are launched. Partnership opportunities, however, may arise from the need to help allies and partners protect their networks and possibly certain high-value pieces of critical infrastructure.

Key Military Cyberspace Issues

Given the nature of cybersecurity threats to US interests, the key military cyberspace questions the next President will confront include the cyber mission force structure, the potential elevation of US Cyber Command to a unified command, the dual-hat role of the Commander of US Cyber Command, the role of the military services, civilian oversight of military cyberspace activities, and partnerships across the US government and with the private sector.

Force Structure

The Obama Administration invested heavily in the creation of a Cyber Mission Force compromised of 133 teams of three types:

- 13 National Mission Teams to defend the nation from a cyber attack of significant consequence;
- 27 Combat Mission Teams to support regional Combatant Commanders with offensive cyber operations;
- 68 Cyber Protection Teams to defend DoD networks and assets;
- 25 Support Teams to provide additional analytic and planning resources to the National Mission Teams and Combat Mission Teams.

US Cyber Command's primary focus over the last several years has been to bring these 133 teams to a level of readiness to execute their missions. Training this force is time-intensive, but Admiral Rogers recently testified that over 90 percent of units should reach initial operating capacity by the target date of FY2018. Even then, however, these units will continue to need additional time gathering operational experience and to manage the inevitable turnover in personnel until the pipeline for new, full-trained, and experienced personnel is stabilized and properly supported by a career management mechanism that captures and sustains cyber talent over succeeding careers.

The next President should assess how these forces are assigned and consider alternate constructs that may reflect the experience of four years of building the cyber mission force. Among others, one consideration may involve how best to balance between preparing to counter geographical vs. technical threats.

National Guard and Reserves

Although the 133 teams of the Cyber Mission Force are essentially an active-duty force, the National Guard and the Reserves can be powerful supplements to the CMF. Indeed, Congress mandated that the Department of Defense examine how the Guard and Reserves could contribute to the national cyber force posture in Section 933 of the 2014 National Defense Authorization Act. The traditional inclination is to consider employing these forces in the aftermath of a cyber intrusion or serious operation. However, the next administration should consider how the Guard and Reserves can be used ahead of an incoming cyberattack to better protect critical assets before an incident. The capability of National Guard units to operate across the range of State (Title 32) and federal (Title 10 and 50) authorities, combined with the ability of the private sector to generate and sustain deep talent in citizen-soldiers/airmen/sailors makes the use of the National Guard and Reserves a cost-effective, high leverage, force for integration and augmentation.

Sub-Unified or Unified Command

As of May 2016, US Cyber Command remains a sub-unified command subordinate to US Strategic Command. Recently, there has been a debate about whether to elevate U.S. Cyber Command to the status of a functional unified command. Proponents of elevation stress that such an arrangement would streamline operational authority between the National Command Authority and the Commander of US Cyber Command, cutting out the middle man (the commander of US Strategic Command). Others express caution that the increase of bureaucracy to operate a unified headquarters staff outweighs the negligible operational impact of elevation.

The original logic of placing Cyber Command under Strategic Command reflected the historical origins of cyber operations and the inherent advantage of leveraging existing capabilities. The National Security Agency has the mission for computer network exploitation and the collection and analysis of foreign signals intelligence under Title 50, but was not authorized to conduct Title 10 offensive or attack missions. Instead, prior to the standup of US Cyber Command, US Strategic Command employed a stand-alone Joint Functional Component Command for Network Warfare (JFCC-NW) for Title 10 offense and a Joint Task Force for Global Network Operations (JTF-GNO) for Title 10 defense. Under this pre-US Cyber Command construct, the Director of NSA was dual hatted as the commander of JFCC-NW and the Director of the Defense Information Systems Agency (DISA) was dual hatted as the commander of JTF-GNO. Both of these Title 10 constructs were rolled into US Cyber Command, preserving subordination of each of these functions to U.S. Strategic Command and the firewalling of Title 10 military operations from the intelligence support provided by NSA.

One reason to elevate Cyber Command is to allow Strategic Command to focus on its core competencies of nuclear deterrence, space operations and global strike. While analysis behind that element of this change is beyond the scope of this paper, the impact that elevating Cyber Command would have on Strategic Command is an important aspect of the decision.

Elevating Cyber Command should also be seen as an opportunity to empower the command with non-traditional authorities it may need to better execute its missions. For example, last year's National Defense Authorization Act included a small test program that authorized Cyber Command (albeit on a limited basis) to bypass the military services and directly acquire capabilities. The inspiration for this authorization was likely the perceived need for agility in capability development and deployment in the dynamic domain of cyberspace. The model tracks the experience of US Special Operations Command, to which Congress granted several unique authorities when it mandated the command's creation in the mid-1980s.

There is no prohibition on granting special authorities to a sub-unified command as Cyber Command as currently structured, so special authorities need not be a function of elevation. However, elevation would reflect the senior leadership's affirmation that cyber operations have become just as crucial to the national defense as the other functional commands and sustain the current permission-to-operate-without-exacting-coordination delegated by U.S. Strategic Command to US Cyber beyond the current personality-dependent situation.

Regardless of whether President Obama elevates Cyber Command before the end of his term, the next administration should evaluate Cyber Command's authorities and ensure it can set its own requirements for acquisition. It should also be authorized and resourced to acquire needed

capabilities as rapidly as possible. In addition to these capability-development authorities, the readiness of the 133 teams of the Cyber Mission Force should drive whether additional recruitment and retention authorities are needed so Cyber Command can attract, develop, retain, and career-track top military and civilian talent.

The Status of the Dual-Hat Commander

At present, the Commander of US Cyber Command is dual-hatted as the Director of the National Security Agency. This arrangement reflects the origins of US Cyber Command from when the commander of one of its predecessor organizations, JFCC-NW, was dual-hatted with the NSA Director. The logic of this arrangement was to empower one individual with the ability to leverage the combined resources of NSA and the uniformed services and pivot quickly between defense, exploitation and attack as needed. Given that the underlying mechanics of these operations were often similar, anointing one individual to conduct full-spectrum computer network operations was compelling.

One area of tension the dual-hat arrangement creates, is that one person – the dual-hatted commander and director – is required to represent two opposing interests in considering an offensive cyber operation: the operational gain and the potential intelligence loss. The responsibility of balancing these equities will only become more challenging as Cyber Command achieves greater readiness and independent capabilities. A system in which operational gain and potential intelligence loss have senior advocates could have advantages. This issue will become more acute as US Cyber Command and the role of cyber operations within the Department continue to grow.

The next President will have the opportunity to review this dual-hat arrangement and determine if the NSA and Cyber Command should be led by different individuals. More than most issues discussed in this paper, this decision has deep, technical issues at stake and should be made based on an analysis of capabilities development and readiness at each institution There is no immediate reason to act, the current arrangement under Admiral Michael Rogers appears to be working well. At the time when Admiral Rogers's appointment expires, it would be worth exploring whether breaking the dual-hat would help these institutions accomplish their missions more effectively.

Beyond the questions of whether and how to convey authorities for acquisition and intelligence collection to a stand-alone U.S. Cyber Command, the issue of the specific relationship between NSA and U.S. Cyber Command will demand significant attention. The Director of National Intelligence and NSA's non-DoD customers will argue strongly for a relationship that does not subordinate NSA to US Cyber Command. The Department will nonetheless still want the relationship to retain the intimacy and collaboration enjoyed under the present scheme.

The Role of the Military Services

While US Cyber Command has the lead for US military operations in cyberspace, the four military services play a crucial role as force providers to the cyber mission force. This is similar to the role they play for conventional forces. The services train national mission teams, combat mission teams, and cyber protection teams, each using its own procedures to organize and train these units. While there are joint training standards, each service is responsible for assigning

individuals to units and getting them into training pipelines to support their eventual Cyber Command missions.

Unless a broader Goldwater-Nichols-like reform movement changes the relationship between the services and the combatant commands, there is no reason to make such a change only for cyberspace. As the services continue to train forces for the CMF, however, it may be worth re-examining how each service recruits and retains top military and civilian performers to exchange best practices. Again, the experience of Special Operations Command in supporting career-long professional development tracks will be a useful model for US Cyber Command. Finally, because each service draws from different communities (from signals intelligence to communications) to create cyber mission teams, the services need to have sufficient resources to ensure these other disciplines do not atrophy at the hands of the cyber mission force.

Civilian Oversight of Military Cyberspace Activities

The Office of the Secretary of Defense (OSD) is the traditional instrument for civilian oversight of the military. For activities in cyberspace, OSD's Chief Information Officer is a civilian partner to Cyber Command's (and the Defense Information Systems Agency's) design of network standards and policies. For acquisition issues, the Under Secretary for Acquisition, Technology, and Logistics is the Department's top decision authority for major system procurement. For operational questions, the Under Secretary for Policy (specifically the Deputy Assistant Secretary of Defense for Cyber Policy) and the Under Secretary for Intelligence provide civilian oversight.

Three years ago, Congress mandated the creation of a Principal Cyber Advisor (PCA) to the Secretary of Defense to serve, among other things, as the focal point for coordination within the Department and to be a single point of contact for Congressional interaction with the Department on cyberspace issues. The details of how the PCA has functioned are mostly not publically available, including what its specific responsibilities have become and how successful it has been at coordinating across the Department's many offices. According to statute, the PCA must be confirmed by the Senate (so an Assistant Secretary or higher in rank) within the Office of the Under Secretary for Policy.

The next President will have the opportunity to review this arrangement to see if it adequately provides the degree of civilian oversight that the Defense Department requires. One consideration may be to propose to Congress that it elevate the PCA to a full Assistant Secretary position to perform the intended coordination and oversight functions. In that sense, this new Assistant Secretary would be similar to the Assistant Secretary for Special Operations and Low Intensity Conflict, which Congress called for as it created U.S. Special Operations Command in the 1980s. Thus, part of the decision about how to best structure civilian oversight needs to reflect US. Cyber Command's continued evolution.

Another balancing act within OSD will be the role of the Department's Chief Information Officer relative to any new Assistant Secretary. The CIO should be organized within the emerging office of the Under Secretary for Business Management and Information, responsible for overseeing the operation and protection of the Department's enterprise systems. A separate, likely Senate-confirmed individual within the office of the Under Secretary for Policy should be responsible for the oversight of military planning in cyberspace and offensive cyber operations.

Despite the common refrain that offense and defense are merely two sides of the same coin in cyberspace, the civilian oversight and coordination functions in OSD are sufficiently distinct to warrant this division of labor.

Partnerships across the U.S. Government

Law enforcement

Despite its growing size and stature within the US defense establishment, US Cyber Command and its components can only accomplish so much on a national level. During the Obama administration, the responsibilities for the Department of Homeland Security expanded to enable better coordination with owners and operators of critical infrastructure. The FBI also emerged as a powerful, operational entity within the U.S. government whose domestic law enforcement authorities and growing technical experience offered a strong complement to externally-focused military operations.

Greater cooperation between the military and law enforcement is not just prudent – it is required due to how the domestic and international jurisdictions dividing the military and law enforcement communities break down in cyberspace. Indeed, cyber operations against the United States using international and domestic infrastructure represent a new form of "lawfare," a term coined over a decade ago to describe how terrorists exploited gaps in U.S. law. As a result, the U.S. military *must* work with counterparts in law enforcement to combat threats that reject the current division of domestic and international labor within the U.S. national security establishment.

One opportunity the next administration may wish to explore is how to use the military services' investigatory offices to bridge the military-law enforcement gap. For example, the Air Force's Office of Special Investigations (AFOSI) has unique authorities through its counter-intelligence mission to undertake domestic forensics investigations, even if the chain of evidence leads them outside of Air Force networks. At present, the limited number of AFOSI agents in the field undertaking cyber-related work limits the extent of cooperation. However, if AFOSI and its Navy and Army counterparts were given increased resources for cyber-related investigations and activities, they could grow into a natural bridge between US Cyber Command and the domestic U.S. law enforcement community.

Intelligence

The need for close partnerships between US military cyber forces and the intelligence community cannot be overstated. For US military forces to be able to prevent or preempt an adversary's offensive cyber operations against the United States, intelligence – no matter the type or source – is critical. Without it, military cyber forces will be confined to a reactive posture.

Previous administrations have provided the resources and organizational flexibility to foster close collaboration between the intelligence and military cyber communities. For the next administration, the opportunity will be to streamline the speed at which information can be shared between intelligence and military communities, as well as from those communities to law enforcement and other institutions that may benefit from specific, threat-based information. Calls for sharing at real-time or near real-time speeds are laudable, and there are undoubtedly obstacles

that can be removed to increase the speed at which some information can be shared between some entities. However, system-wide real-time sharing is probably still a distant possibility.

Partnership across Private and Public Sectors

Finally, the protocols and thresholds governing DoD defense of civilian infrastructure must be further defined and exercised to ensure efficient and effective transitions between the various roles assigned to private sector and government organizations. The ends of the spectrum (peace and tranquility on the one end and state-to-state conflict on the other) are well understood and similarly well-practiced. Experience navigating the transition between the two is virtually non-existent. Given that sharp transitions favor the aggressor who chooses the time, place, and pace of action, an integrated and coherent defensive scheme is the best mitigation, complemented by an overlay of collaboration amongst the parties owning, operating and defending cyber infrastructure. This reality calls out for a collaboration between the private and public sectors. A simple division of effort, however attractive, will not suffice. Information sharing that enables shared situational awareness and rapid, fluid shifts of defensive efforts will be a key enabler. Privacy and security will be difficult to align but must be the goal to ensure an enduring solution that works across sectors and national boundaries.

Cyber and Deterrence—the Military-Civil Nexus in High-End Conflict

Introduction and Executive Summary

This paper analyzes cyberspace's role in deterrence and defense—and specifically the military-civil nexus and the relationship between the Department of Defense (DoD), the civil agencies, and the key private operational cyber entities, in particular the Internet Service Providers (ISPs) and electric grid operators. The focus of the paper is on high-end conflict including actions by an advanced cyber adversary, whether state or non-state, and not on the "day-to-day" intrusions and attacks as regularly occur and are generally dealt with by governmental agencies and the private sector without military involvement. High-end conflict can be expected to include attacks within the United States homeland as well as in forward theatres.

Earlier this year, the Administration issued PPD-41, "Cyber Incident Protection," setting forth cyber security incident roles and missions for federal agencies but with no reference to the Department of Defense.[17] By contrast, the *DoD Cyber Strategy* provides that DoD will be prepared to "defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence."[18] Certainly, in a conflict where an adversary will utilize cyber as part of an overall military attack, the DoD will necessarily play a major operational role. This paper discusses what that role should entail.

In a high-end conflict, the military will rely heavily on the availability of the telecommunication and electric grid networks, and those networks--including abroad--will likely need the assistance from the military to remain operationally effective. Understanding cross-sectoral dependencies and potential cascading effects from attacks will be crucial. Accordingly, to achieve deterrence and/or successful defense with respect to such a conflict or potential conflict situation, particularly against high-end cyber adversaries, the military, civil authorities, the ISPs and grid operators will need to work closely together both prior to and during the conflict. This will be true both inside the United States and in the forward theatres where conflict is likely to occur.

The paper is organized in two parts. The first, and more extensive section focuses on requirements necessary inside the United States. The second discusses requirements for forward theatres, building on the analysis for the US territory and the authors' previous paper "Cyber, Extended Deterrence, and NATO."[19]

The broad conclusion of the paper is that effective planning and operations require two overlapping sets of requirements to be undertaken:

---

[17] Presidential Policy Directive/PDD 41, "US Cyber Incident Coordination," https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. See also, U.S. Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 30, 2016. The draft National Cyber Incident Response Plan, which will implement PPD-41, contains references to defense activities, but places DHS and other agencies in the lead even in the event of a significant cyber incident, https://www.us-cert.gov/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf.

[18] U.S. Department of Defense, *DOD Cyber Strategy* (2015), at p. 14, [hereinafter *DoD Cyber Strategy*], http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[19] Kramer, Butler, Lotrionte, "Cyber, Extended Deterrence, and NATO," (2016), http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf.

- **The military needs to develop a concept of operations that allows it to determine the required support from the ISPs and the electric grid in a high-end contingency (such as defense of the Baltics) and to provide the basis for a prioritized approach to cyber protection, resilience, and recovery of those networks**. In order to prioritize mission-essential networks and industrial control systems that are critical for responding to regional crises, coordination with civil authorities, the ISPs and electric grid operators both prior to and during a crisis will be necessary.

- **The civil authorities, the ISPs and electric grid operators need to develop contingency planning to elucidate the type of assistance they are likely to need from the military in order to provide the protection, resilience, and recovery necessary to maintain adequate telecommunications and grid operations for the nation in the event of a high-end contingency.** The grid and ISP operators have unique knowledge of their specific system architecture and restoration plans and; therefore, they are the best experts to convey that information to the military so the military is ready to actively support their efforts both during an attack and for post-cyber attack restoration. Without this foreknowledge about the specific systems, DoD personnel who undertake to assist during a crisis would be ineffective and could in fact cause harm to the systems and contribute to other adverse consequences.

To accomplish these objectives in the United States, six steps need to be undertaken:

1. **Contingency plans for military, civil authorities, ISP and electric grid operator interactions**. These plans must be established for a high-end contingency through the use of an effective planning process supported by regular exercises and detailed playbooks that are routine in other emergency scenarios such as storms, fires or earthquakes.

2. **Clear chains of command for a high-end contingency need to be established between the civil authorities and the DoD and within the DoD itself**. This should include an operational mechanism needs to be created to include the ISPs and the electric grid to allow prompt and responsive actions. To remedy existing disconnects between the DoD and other departments and to allow for proper interaction with the ISPs and grid operators in the context of a high-end contingency, Congress should consider creating a requirement for "unified cyber actions" along the lines of what the Goldwater-Nichols Act established for the DoD, requiring joint actions among the four services for war fighting purposes.

3. **Undertake actions in advance of a high-end attack in order to establish the greatest likelihood of effective protection, resilience, and recovery.** Numerous analyses have determined that to generate desired results defenders cannot wait for the actual attack. Among other important steps prior to conflict, intrusions need to be blocked as much as possible, malware needs to be removed, and capabilities for maintaining data integrity, confidentiality and availability need to be built and exercised. Critical to this effort is the use of a variety of adaptive resilience techniques, ranging from diversity and redundancy to moving target defenses and deception.[20] All these resiliency features require development and implementation prior to conflict. Not all attacks can be protected against, but their effects

[20] Harriet G. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," The MITRE Corporation (2010), https://www.mitre.org/sites/default/files/pdf/10_3301.pdf.

can be mitigated if steps are taken in advance. DoD can utilize the knowledge generated in the defense of its own networks to assist defenders, and undertake research and development through the Defense Advanced Research Projects Agency and other DoD applied research and development (R&D) activities to provide advanced capabilities.

4. **The roles of the National Mission Teams (NMTs), currently being established by Cyber Command to respond to cyber attacks of significant consequence, and the National Guard (NG) must be developed and clarified.** NMTs and NG missions during an attack should be developed, specifying how they will interact with ISPs and grid operators. NMTs and the NG will not have the degree of expertise that ISP and grid operators have in their respective domains, but a combined effort utilizing exercises and modeling can establish tactics, techniques and procedures for operating in a degraded environment. Additionally, NMTs and the NG should operate not only once a high-end attack has begun, but should help support actions prior to such an attack that will enhance protection, resilience and recovery of the ISPs and the electric grid if an attack occurs. In addition to substantive planning, operational legal authorities must be clarified before an attack occurs. Moreover, a determination should be made whether the capabilities of the active force and the Guard are sufficient or whether they need to be supplemented by private sector cyber security expertise, working under government direction and control in connection with high-end contingencies or in direct support to the ISPs and grid operators. For both conflict and restoration operations, such private sector skilled personnel may be necessary especially if the NMTs and NG were needed to give direct support to DoD in a time of crisis. Any private sector personnel will need to be familiar with the specific operational technology networks, software applications and protocols of the specific critical infrastructure.

5. **DoD should establish programs and funding to support resilience and recovery.** The US Government (USG) should leverage the National Defense Production Act to ensure that readiness reserves in hardware and systems exist for critical infrastructure providers as they reconstitute/recover.[21] The DoD could provide a contractual program for the purchase of key infrastructure components. Companies who participate could be further incentivized through payments and limited liability protection to provide greater levels of security to their industry supply chain and vendor management processes and to adopt best practice secure engineering and better engineered products.[22] DoD funding could also support the Department of Energy (DOE) efforts contemplated under the Strategic Transformer Reserve of the Fixing America's Surface Transportation Act (FAST Act).[23]

6. **Prior to conflict, undertake expanded fusion efforts, largely by civil authorities, including intelligence, cyber, financial, law enforcement and other capabilities to disrupt adversarial cyber planning and operations.** Offense will be a key element of effective operations. Campaign planning should include courses of action to respond to so-called hybrid warfare, including cyber-enabled "flexible deterrent (and response) options" so

[21] Melissa E. Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," Chap. 6 in *Securing Cyberspace: A New Domain for National Security*. Queenstown, Md.: Aspen Institute, February 2012.
[22] The Civil Reserve Air Fleet Program (CRAF) in fact provides for DoD inspections to ensure that appropriate engineering and maintenance standards are met.
[23] Fixing America's Surface Transportation Act, P.L. 114-94, December 4, 2015 [hereinafter the FAST Act]., https://www.gpo.gov/fdsys/pkg/PLAW-114publ94/pdf/PLAW-114publ94.pdf.

that commanders will have a full spectrum of options to utilize if the President determines it appropriate. In the event of conflict, cyber capabilities can be used against an adversary, targeting not only adversary cyber but also military capabilities such as sensors, communications, logistics and military supporting infrastructures.

In forward theatres, effective operations will require all of the foregoing to be undertaken including contingency planning, clear delineation of command chain, clarity on the role of cyber teams, identification of prior actions to enhance protection, resilience and recovery, and use of offense. However, as the United States will be operating as part of an alliance or organized coalition, cyber requirements will have to be coordinated and undertaken with allies and coalition partners. Accordingly, in addition to the specifics noted above, four additional elements will be key: the US should act as a "cyber framework nation" to help support national capabilities; operational partnerships should be created between and among the military, civil authorities, the ISPs and grid operators in the host nation; standards and procedures similar to those undertaken in the US should be adopted by host nations; and cyber tools should be part of the military war-fighting effort, to disrupt adversary cyber operations and military capabilities including sensors, communications, logistics, and war supporting critical infrastructure.

Raising the Cost to the Adversary

Margie Gilbert

Bobbie Stempfly

Introduction

The impact of cyber intrusions into US systems has never been higher. While cyber defensive measures are important, it is time to raise the cost to the adversary through a range of remedies proportional to the threat and actors who threaten the health and vitality of cyberspace. Ideally, we want the adversary to conclude that the cost is greater than the payoff.

Several challenges immediately arise. First is the diversity of actors and motivations in play – consequences that may deter one may be ineffective against another. Second is the difficulty of attribution in cyberspace where anonymity is easily derived by hiding amongst large populations or active efforts taken by aggressors to employ readily available cloaking measures designed to thwart attribution and attendant consequences.

Against this backdrop, the CSIS Task Force recommends a framework that offers a range of remedies along a continuum of passive to active measures industry and government can undertake to impose costs on aggressors.

Highlights of the framework include:

- **Discrete options and interdependencies.** The framework showcases discrete options that may be employed in isolation while suggesting interdependencies intended to allow any one initiative to leverage the benefits of another. Two examples of these interdependencies suggest the manner in which synergy may be achieved more broadly:
    1) Foundational work invested in hardening software and hardware (traditional information assurance) significantly "raises the cost" for low capability hackers while establishing a basis for improving identification, attribution and action against considerably more capable aggressors.
    2) Initiatives that address policy, norms setting, and liability protection can motivate, empower and strengthen the hand of individual defenders.
- **Spectrum of options.** The options themselves are laid out along a spectrum that ranges from passive to proactive activities. Defenders can undertake actions largely within networks and systems under their control, while the latter spans from actions that directly respond to aggressor actions at the point of discovery to actions taken to impose consequences on aggressors in their home environment.
- **Mapping options to level of attribution.** The degree of attribution required to implement the options presented varies. Passive measures require no attribution while active ones require a degree of attribution that is supported by the foundational activities suggested above.
- **Incorporating parallel action and cooperation.** While the actions we would deter are set in cyberspace, we have been careful to generate a set of recommendations that can be worked alone or together, derived from the authorities and capabilities of private citizens, diverse sectors, and government(s).

The Cyber Environment

The cyber environment includes threat actors and influencing factors. If we plan to raise the cost to the adversary, we need to know **who** the adversary is (attribution), **why** they want to attack us (motivation and intent), **what** capabilities the adversary has against our network and

data, and ideally **how** and **when** they plan to attack[24].

The Who and Why

The below categories of cyber actors, i.e., those who conducted (or will conduct) the attack, are most commonly accepted by US cyber policy experts:

Cyber Actor	Description
Nation State	The actor is employed by the government of a nation-state, e.g., China
Organized Crime	Criminals that engage in illegal activity, often for monetary gain
Activists	An actor that performs attacks in order to draw attention to a cause (such as free speech or human rights), or hinder the support of a cause
Terrorist	Actor carries out an attack designed to cause alarm or panic with ideological or political goals, affiliated with a terrorist organization
Individual (Lone Wolf)	A specific person acting on their own accord—possibly motivated by, but not affiliated with—an organized group

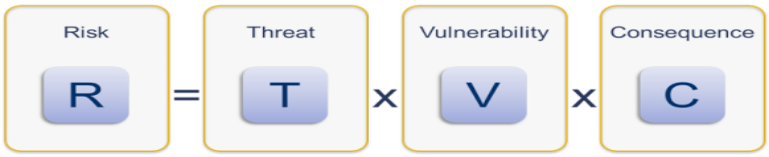
The What

Two core vulnerabilities in our cyber systems are the network and data. Many attack vectors exist within these two areas, such as denial of service, extortion, or data theft. For example, the 2015 OPM breach compromised personal data of more than 21.5 million people. Reference Appendix A for additional examples of what can be targeted in cyber attacks.

The How and When

This information tends to be more elusive in understanding cyber adversaries, unless you have intelligence into their innermost planning cycle. That said, if you build a profile of your adversary (understand the adversary that wants to attack your network and data) then you can start to build a defensive posture.

Another way of looking at the cyber environment is through a commonly accepted risk equation. The US Government often includes "intent" as another variable, because it denotes the resolve and determination of an adversary to carry out the attack, e.g., terrorism.



This equation introduces the concept of "consequence," the effect of the cyberattack. This can range from disruption of communications to destruction of data. Reference Appendix B for additional examples of effects from a cyberattack.

[24] Attack in military context could be considered an act of war, but media tends to use the term synonymously with intrusion or exploitation.

The tactics, techniques, and procedures (TTP) used in a cyberattack often take advantage of vulnerabilities in technology and the human, and can range from basic social engineering to advanced persistent threats (APT). Referencing mostly US data, one prominent report[25] highlights the most common attack vectors, to include Web applications, point-of-sale systems used in stores, and phishing campaigns using social engineering to entice users to click on infected email, attachment, or web link. The effects or consequences include theft of intellectual property, trade information, and legal documents (often linked to nation states) and personal credentials or financial data (often linked to criminal elements). Trends have changed little over the past years, except for increased speed and ease for cyber adversaries. Table 1 is one example, showing threats to the private sector, of areas impacted by cyber threat actors.

	Nation State	**Organized Crime**	**Activists**	**Terrorists**
Victim Industry	Finance Energy IT & Comms Transportation	Finance Health IT & Comms	Media Government IT & Comms	Media Public Sector IT & Comms
Region of Operation	Eastern Europe East Asia	Eastern Europe Africa South America	Europe North America	Middle East Africa Southeast Asia
Common Actions	Espionage Exploitation Attacks	Extortion Exploitation	Public Disclosure Propaganda	Attacks Propaganda
Targeted Assets	Networks Data Systems	Networks Data Systems ATM POS	Networks Data Systems Web Apps	Networks Data Systems Web Apps
Desired Data	Credentials Internal Data Trade Secrets System Details	Credentials Bank Accounts Payment Cards	Credentials Internal Data	Personal Info System Details

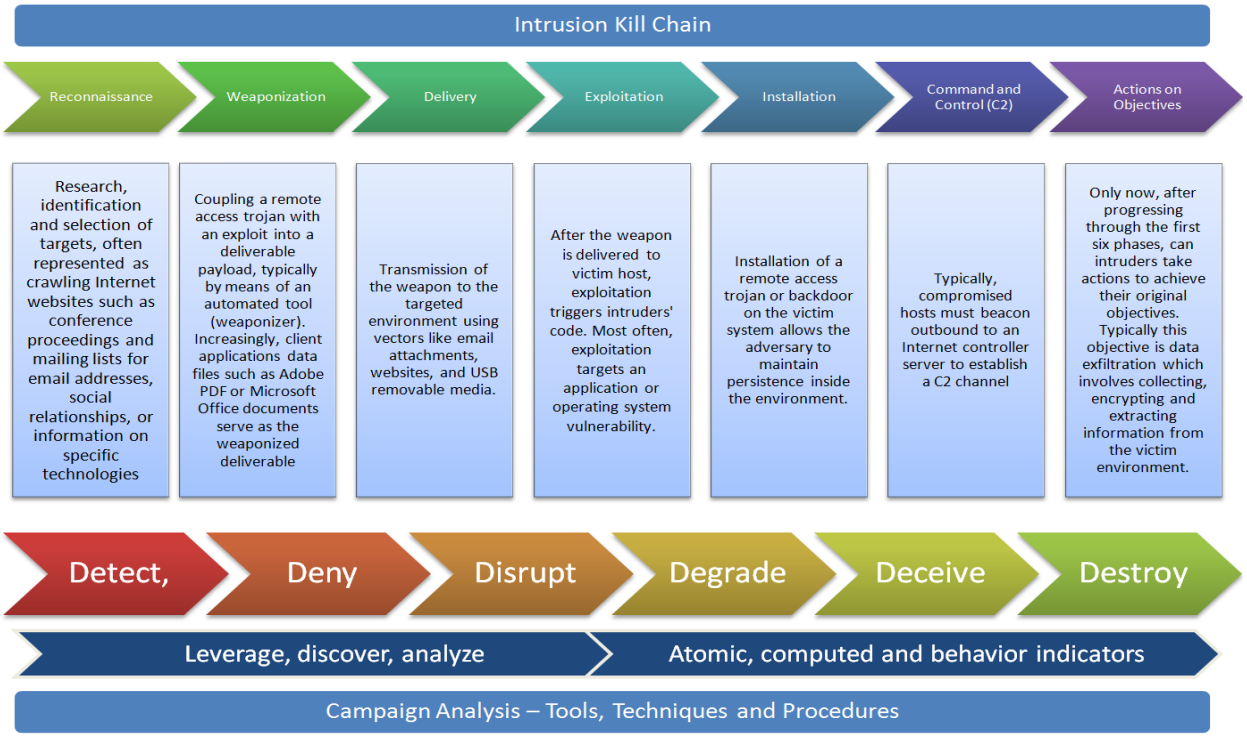
Similar reports are issued across the US Government and industry to assess the cyber threat environment using the aforementioned attributes. With the *who, what, why, when,* and *how* established, let's now consider the spectrum of response options available.

The Spectrum of Cyber Response Options

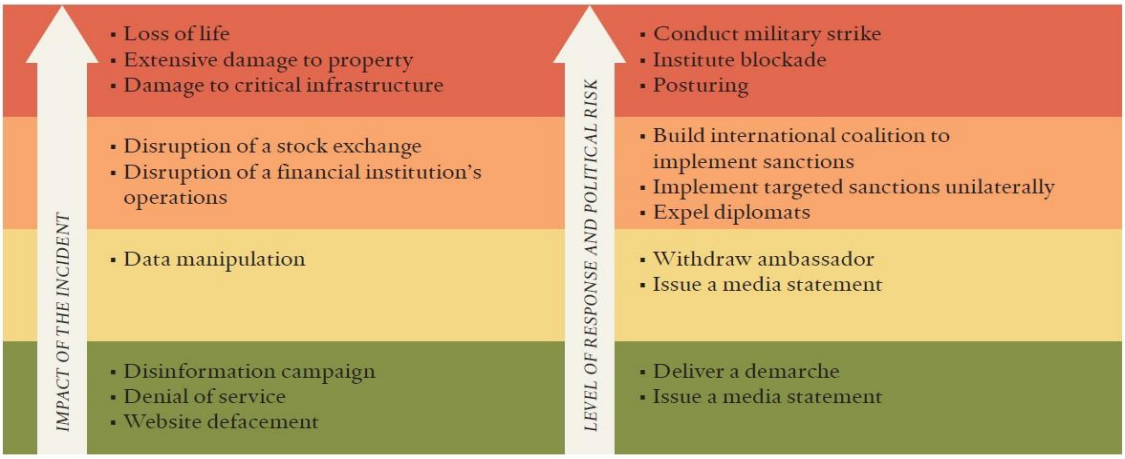
There is a wide range of cyber response options. One military perspective focuses on the cyber intrusion kill chain, is presented below.[26] Its premise is based on the evolution of APT as an intelligence-based model. Appendix C provides another view from the US defense mission.

[25] Verizon Data Breach Investigations Report, 2015

[26] "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", E Hutchins, M Cloppert, R Amin, Mar 2011



Another example looks at national policy options and outlines the different levels of state power that can be applied in response to escalating levels of a cyber incident. Across the response spectrum there will be inherent political and legal risks associated with each decision, and risks increase as the level of the response increases.[27]



While few examples exist of response options taken in and through cyberspace, it is reasonable to assume that such options will be (or already have been) developed and employed. To preclude the ambiguity and attendant chaos that may result from the rise of mercenary or vigilante actors, policy and law must ensure that cyber options are developed and employed with three considerations in mind:

[27] "Developing a Proportionate Response to a Cyber Incident", Tobias Feakin, International Cyber Policy Centre, Australian Strategic Policy Institute, Aug 2015

1. Cyber options considered and employed in the context of all instruments of power (rather than as stand-alone options employed in cyber-on-cyber engagement);
2. Cyber options meet the same standards of necessity and proportionality as other instruments of power; and
3. Policy and law clarify which the US Government reserves cyber response options for employment, and which are suitable for use by individuals and the private sector. Current definition of roles and responsibilities as defined in the 1986 Computer Fraud and Abuse Act and other policies need updating to reflect current circumstances and the middle ground of self-defense in shared spaces (i.e., global commons) amidst the dynamism and ambiguity of cyberspace.

Recommendations for the Next Administration

The impact of cyber intrusions into US systems has never been higher, and while cyber defensive measures are important, it is time to *raise the cost to the adversary* through a range of remedies that are proportional to the threat and actors who threaten the health and vitality of cyberspace. Ideally, we want the adversary to conclude that the cost is greater than the payoff.

The recommendations below only address those elements that have the most potential to impose costs to cyber adversaries. These are designed to impose a cost to the adversary, simply put "let the adversary spend $1 attacking us, and we will cost them $100 thanks to our multi-pronged approach." For those seeking a wider spectrum for cyber defense, reference Appendix C where other responses more appropriate to 'instruments of national power' may be warranted.

Options for Raising the Cost to Cyber Adversaries

Recommendation	Implementation	Example
Frustrate the effective monetization of stolen data/credentials **Pros** • Reduced attacks • Disrupt adversary networks **Cons** • Escalated retribution	1. Reduce the "quality" of stolen credentials available in the underground economy. Foment uncertainty amongst criminals dealing in their trade.[28] 2. Increase countermeasures to target the money mule; cash out infrastructure of criminals and their use of virtual currencies to transfer or launder illicit funds.[29] 3. Seize/freeze assets associated with cybercrime via cyber sanctions and other tools.	1. Innovative joint LE & bank operations to generate and distribute fake 'stolen' credit card numbers and account login credentials across criminal forums. 2. Identify and exploit the weaknesses in the criminal's existing economic model. 3. EO on cyber sanctions (this already exists, but there are implications to its use which haven't been addressed yet).
Divert Adversary Resources towards Defense versus Offense	1. Divest and disassociate critical data.	1. Spread targeted data across multiple servers.

[28] This may need DOJ opinion to support industry defending their intellectual property
[29] Widen scope of Bank Secrecy Act/ FINCEN/Safe Harbor for exchanging this information to address non-bank financial institutions

Pros • Reduced adversary attacks • Attack diversion **Cons**	2. Target population problems. 3. Setup single corporation designed to draw attention to them.	2. DDOS CN gaming-related infrastructure – internal effect – causes government to lose "face" with population. 3. Non-profit security firm publishes reports, bad IPs, etc.
Paralyze Adversary Infrastructure **Pros** • Reduced adversary capacity **Cons** • Escalated retribution	1. Know adversary TTPs and tailor the response for most impact. 2. Set up bogus or old exploits that keep adversary busy and guessing.	1. CN is very rigid; RU will shut down at one knock at the door 2. Port 24 scans that try to connect to Command & Control servers
Enable US Companies to Respond in Non-destructive Manner **Pros** • Stops loss of IP • Shareholder confidence **Cons** • Lost profits • Lost market share to China	1. Letter of Marque + tacit consent from AG that US Companies won't be pursued for non-destructive cyber response. 2. Stand Your Ground or Castle Defense law for cyberattacks (e.g., State law). 3. Provide threat data to support supply chain decisions.	1. Company pursues adversary. 2. Company can scan the address that hacked into their system; look to see if their data is there; pull their data back. 3. Anonymize source feeds on foreign malware and threats.
POTUS Statement of Intent followed by Action **Pros** • Regain credibility and respect • Reinforce international norms **Cons** • Consistent USG messaging • Ability to respond quickly • IC/DOD equities impacted	1. New POTUS sets tone early. 2. NSC Structure – Action for Incident Response. 3. Respond to exploits quickly.	1. Press statement: "US will not tolerate cyber attacks." 2. Immediate restructure of the position and staff (PDD). 3. USG response for USG attack; Industry response for Industry attack.
Reduce Anonymity with User Authentication/Attribution **Pros** • Proven biometrics exist **Cons** • Adapting acquisition process • Long lead time to adopt	1. Multi-factor authentication ("mantrap" defense) - encourage strong authentication for users within public and private organizations when accessing restricted resources.	1. Require attribution for access, e.g., biometrics.

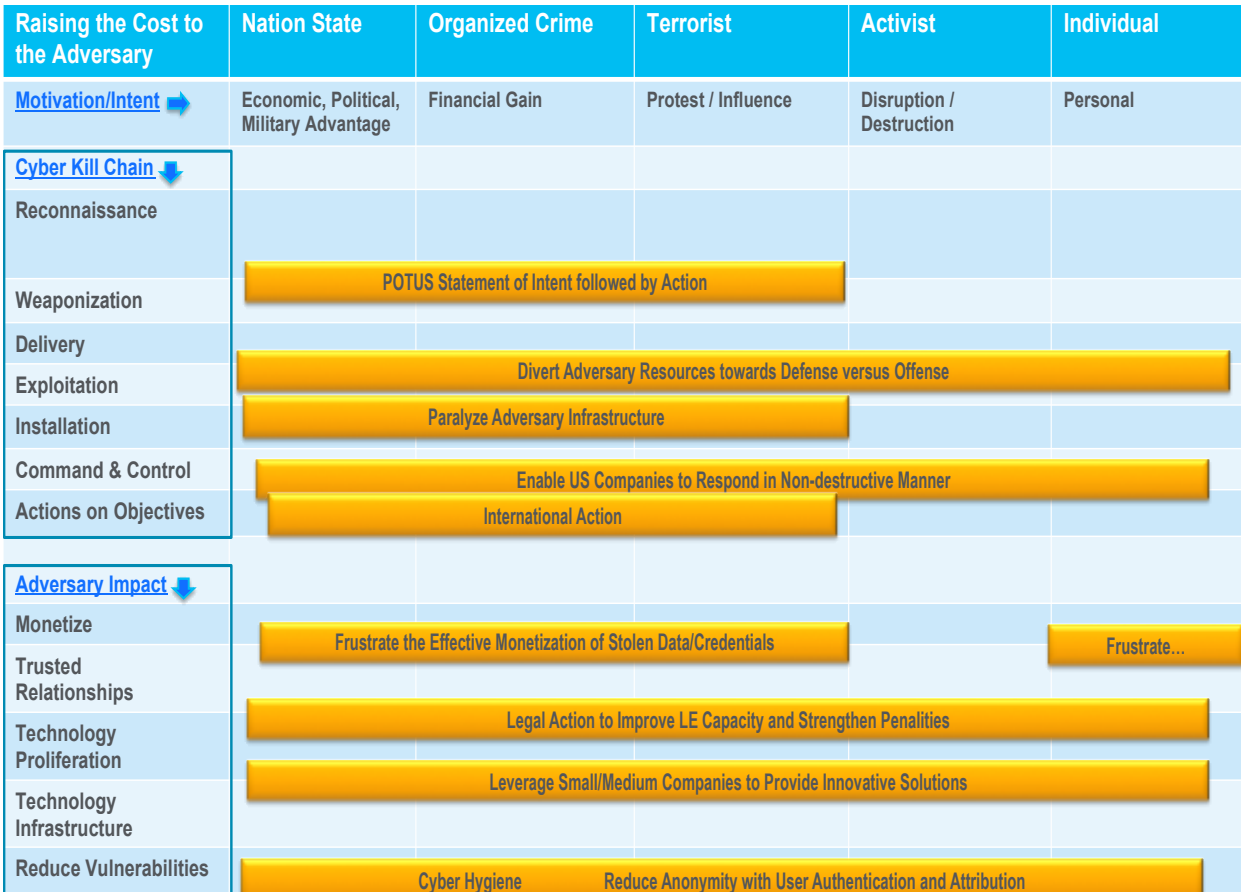
Cyber Hygiene[30] **Pros** • Proven approach **Cons** • Adapting acquisition process	1. NIST Framework 2. Whitelisting 3. Rapid Patching 4. Limited Administrative Privileges 5. Encryption (transit & at rest)	1. Make "cyber accounting" standards much like GAAP to describe to a company's leadership/board the "cyber balance sheet." This can support the hygiene objective and use market forces to drive improvements within a company or their supply chain.
Leverage Small/Medium Companies to Provide Innovative Solutions* **Pros** • More innovative options • Increases agility to adopt **Cons** • Rigid acquisition process • Ability to scale	1. Employ new technologies, tactics, techniques to engage the adversary.	1. Industry as cyber threat data provider to USG; data aggregator; bulk data analytics.
Legal Action to improve LE capacity, strengthen penalties **Pros** • Sets precedent • Validates older laws today **Cons** • Long lead time for action	1. CFAA 2. RICO 3. US Uniform Trade Secrets Act 4. Criminal Indictments	1. Deputize industry for certain functions.
International Action **Pros** • Reinforce int'l norms **Cons** • Long lead time for adoption	1. World Trade Organization 2. United Nations	1. Digital Assets treatment in International law. **

The table below maps the aforementioned options against cyber actors, their motivation or intent, and cyber responses to provide a visual perspective of the potential impact for raising the costs to the adversary. We seek the outcome where the adversary concludes that the cost is greater than the payoff of continued cyberattack.

[30] James A. Lewis, "Raising the Bar for Cybersecurity," Center for Strategic and International Studies, February 12, 2013. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

***** USG decision-makers rely on large companies to recommend solutions that crowd out other companies that can't scale or compete on large contracts.

****** Negotiate to get standing in international law for a digital asset. Today only physical assets have clear standing if attacked. It needs to be clear that attacks (vs. espionage) are a violation of US sovereignty. Nations have a responsibility for their actions and actions taken from their sovereign space upon other nations, but this does not seem to apply to digital assets.



Conclusion

Over the past years, the Administration has proposed initiatives such as the Comprehensive National Cybersecurity Initiative (CNCI) and investments across the Federal Government. Federal partnerships with the private sector have faltered, leaving industry mostly alone to deal with cyber theft of intellectual property, whether from nation states or cyber criminals. Researchers have tried for an equal number of years to account for actuarial impacts to businesses, while the impact to the US gross national product remains widely speculated.

Raising the cost to adversaries should be an urgent option that complements other instruments of national power. The United States does not widely control critical infrastructure sectors (unlike other countries, such as France, China, Russia, Iran), and as a result US industries are frequently alone to deal with cyber theft of intellectual property and cyberattacks against infrastructures owned and operated by the private sector. What recourse does the private sector legally have to deal with cyberattacks to their systems and core business? What can the next Administration do to support what many believe are industry rights for 'self-defense' against cyberattacks? The Administration must provide a framework to allow proportionate response to attackers, absent the ability of the Federal Government to protect or respond on behalf of national interests. This paper provides one component of that framework.

APPENDIX A – What Can Be Targeted in Cyber Attacks[31]

Category	Description	Examples
Administrator Accounts	Accounts used to manage system/network resources and services	DNS accounts, server credentials
Social Media Accounts	Accounts for social networking and microblogging	Myspace, Facebook, Twitter, Tumblr
Email Accounts	Email addresses and accounts	Employee email accounts, Gmail accounts
Financial Accounts	Accounts related to banking, trading, payment cards, or any other financial service	Banking credentials, bitcoin wallets, tax accounts
Customer Accounts	Accounts used to purchase/manage services, and facilitate billing (like cell phone or utility accounts)	FedEx accounts, Adobe accounts, health insurance accounts
User Accounts	Accounts used to access a service (Forums, gaming platforms, news sites)	WhatsApp accounts, YouTube accounts
Cloud Account/Single Sign On	Accounts connected to cloud services	iCloud accounts, Google Drive accounts
Point of Sale Systems/Software	Refers to the area of a store where customers can pay for their purchases. The term is normally used to describe systems that record financial transactions. This could be an electric cash register or an integrated computer system which records the data that comprises a business transaction for the sale of goods or services.	Includes all parts of the system, customized hardware, scanners, electronic cash registers, touch screens
Storage Devices /Removable Media	A device for recording or storing information.	USB storage devices, hard drives, CDs and DVDs, tape backup
Medical Equipment	Medical Devices and equipment specific to the healthcare industry	Pacemaker, insulin pumps, any wireless medical devices
Consumer Electronics /Home Appliances	Electronic equipment intended for entertainment, communications, office productivity, and home electrical/mechanical machines.	TVs, gaming consoles, Apple TV, Bluetooth and GPS devices
Network Equipment	Devices that facilitate the use of a network.	Routers, switches, firewalls
Network Resources	Devices that provide services to end users over a network.	Printers, fax, video conferencing systems, server hardware
Desktops/Laptops		Personal computers, employee computers and business workstations
Vehicles/Vehicle Computer Systems	Electronic Control Units (ECUs) and other microprocessors used in automotive	Vehicle anti-theft systems, vehicle electronic control unit, vehicle sensors
Industrial Equipment	Equipment used in manufacturing, energy, and utilities.	Industrial Control Systems
Banking Equipment	Equipment specific to the banking industry	Automated Teller Machines (ATM/ABM), teller terminals, currency dispensers, encoders, cash processing equipment

[31] https://www.surfwatchlabs.com/threat-categories#Target

Security Systems	Security devices, access-control and alarm systems	Cameras, bio-metric scanners, and electronic locking devices
Facilities	Data/call centers, commercial or industrial buildings, housing	New York EU office, nuclear installations
Payment Cards	All banking cards	Credit and debit cards, transit cards, loyalty program cards.
Firmware	Hardware embedded control software	
Operating Systems	All desktop, laptop and server operating systems	Microsoft Windows, OS X, Linux
Mobile Operating Systems	All mobile operating systems	Android OS, iOS, BlackBerry OS
Mobile Applications	All mobile applications regardless of function	BlackBerry Messenger, Angry Birds, Google Play
Web Browsers	Browsers and browser add-ons/plug-ins	Internet Explorer, Google Chrome, Firefox
Entertainment Software	Software used for leisure such as media players, video games, and gambling software	QuickTime, Windows Media Player, iTunes, Call of Duty
Communications Software	All remote access, file exchange (FTP clients), and messaging software clients including email clients and instant messaging/chat	Outlook Express, Foxmail, FileZilla, Yahoo Messenger
Productivity Software	Word processing, database, spreadsheet, and all other office/end user productivity applications	MS Office, Photoshop, Adobe Acrobat
Financial Software	Banking software, Bitcoin software and electronic trading software	ClearPort, FOCUS IV, TradeFortress
Development Software	Application and web development software, programming software and APIs	Java, Adobe ColdFusion, Jboss Application Server
Management Software	Website back-ends, administration software, protocol servers (FTP, HTTP), enterprise security management software, inventory and access control software	Apache, Exchange Server, IIS, vSphere Update Manager
Industrial Software	Industrial control and distribution software, construction and computer-aided design software, production and manufacturing software	AutoCAD, Automated Identification Systems, SCADA
Security/Utility Software	Antivirus clients, security software clients (end user programs), and system utilities	Encryption software, iTouch, MacUpdate, McAfee anti-virus
Cloud Services/Applications	Anything-as-a-Service. This category also includes applications hosted on websites, web 2.0, HTML5 and ASP apps.	Amazon Cloud Drive, iCloud, Evernote, Dropbox, CryptoCat, Pandora, Talkr
Content Management Systems	Website management software and plugins	WordPress, Joomla, Datalife
Data	Digital assets, includes documents, records, database contents, intellectual property, cred card information, PII, account credentials	Electronic health records, source code, customer data, SMS messages
Search Engines	Search engine related targets	Bing, Google Bot, Graph Search
Individuals	Persons' names, and pseudonyms	Michelle Obama
Customers/Clients	Persons or organizations that purchase/manage goods or services from a business. Keywords: investors, guests, shoppers.	Russian banking customers, Sebastian Corp. customers, Westin Hotels & Resorts guests

Patients	Persons receiving or registered to receive medical treatment	Medicaid clients, UnityPoint Health patients
Employees	Persons employed for wages or salary, includes non-official government employees. Keywords: staff, executives, administrators, coworkers, aides	US military personnel, White House employees, University of Maryland staff
Students	Someone who attends an educational institution (includes alumni - a former student)	University of Maryland, College Park students, University of Delaware students
Users	Persons that utilize a service or system. keywords: visitors, readers, players, owners, subscribers	Cake Poker users, Forbes website visitors, Microsoft Office users, Netflix users
Communities	Countries, cities, towns, regions. Keywords: residents, citizens	People of West Papua, Middle East countries
Group Members	Organization members/volunteers, threat groups (hacktivist/hacking/APT groups), and groups of individuals with no organization. keywords: prisoners, activists, fans	APT1, Syrian Electronic Army, LulzSec hacktivists
Government Officials	People elected or appointed to administer a government	Turkish Prime Minister, Ukrainian parliament members, Members of the Ukrainian Parliament
Wireless Networks	Any wireless local area network (WLAN), usually providing a connection through an access point to the wider Internet. Includes other wireless tech. like satcom and terrestrial microwave.	Airport Wi-Fi networks, Wi-Fi access points
Cellular Networks	Radio networks for mobile transceivers (phones, pagers, etc.)	3G/4G/LTE networks, GSM telephone networks
Government/Military Networks	Networks owned and operated by government and military entities	German National Data Center, CENTCOM's computer system, Australian Federal Police networks
Telecommunications Networks	High speed, high capacity, long-distance networks consisting of switches, cables, satellite, wireless transmitters and antennas which support data communications between smaller networks.	International communications links, Ukraine telecommunication systems, Indosat networks
Financial Networks	Networks owned and operated by financial organizations, included financial private networks	Markets, exchanges, Flexcoin networks, HBGary Federal networks
Private Networks	Networks owned and operated by businesses and other organizations	Boeing Company system, Boone Hospital Center networks, enterprise environments
Public Networks	Networks available to anyone	The internet, TOR, IRC
Domains	Generic and country-code top-level domain names as well as second and third level domain names	.com, .edu, .gov.nl
Infrastructure and Utilities	The physical components of interrelated systems providing commodities and services essential to enable, sustain, or enhance a society. This category includes networks supplying a community with electricity, gas, water, or sewerage.	Critical infrastructure, gas and oil pipelines, electric power, water systems
Websites	A public site for a company/business or any other entity. Frequently the target of defacements.	Walmart.com, google.com, and all other websites.

Forums	An online discussion site where people can hold conversations in the form of posted messages.	Ubuntu forum, NASDAQ forum
Blogs	A discussion or informational site published on the web.	Skype's Official blog, personal blogs, WordPress Blogs

APPENDIX B – What Can Happen as a Result of a Cyber Attack?[32]

Category	Description	Examples
Data Stolen/Leaked	When information is illegally copied or taken from a business or other individual. Includes all data types other than Personal and Financial Information.	Intellectual property, such as design documents, sensitive data, such as source code and military technology, user data, such as documents and photos, and other records.
Personal Information Stolen/Leaked	When any form of personal information is illegally copied or taken from a business or other individual.	Includes personally identifiable information (PII), such as social security numbers, protected health information (PHI), such as medical records, and contact information, such as home addresses and telephone numbers.
Financial Information Stolen/Leaked	When financial information is illegally copied or taken from a business or other individual. Commonly, this information is credit card information, online banking credentials and any other financial account information.	Includes payment card data such as credit card numbers and track data, bank account information, and financial records, such as transaction records.
Credentials Stolen/Leaked	When account credentials are illegally copied or taken from a business or other individual.	Stolen SSL keys, stolen file transfer protocol (FTP) credentials
Account Hijacked	Account hijacking is a process through which an individual's email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker.	Often time this will include things like the hijack of a Facebook or Twitter account but can include bank accounts/bitcoin wallets, any instance where an account has been accessed or taken over by a hacker.
Intercepted Communications	Interception of signals, whether between people or from electronic signals.	Electronic surveillance, compromised emails, eavesdropping
Data Altered/Destroyed	The process of destroying or altering data stored on all forms of electronic media - possibly results in making the data completely unreadable or inaccessible.	Examples: deleted database, ransomware encrypted files, altered DNS entries, altered grades
Damaged Reputation	Often related to times when accounts are taken over and used them to spread slanderous / misinformation that effects the reputation of an individual or company.	The hacking of an antivirus company or security company may affect the reputation of how well that company can secure their customers.
Financial Loss	Money has been stolen, or the net result has a financial impact.	This can include hacking into bank accounts to steal money or any hacking incident that costs a company money in fixing the issue/or costing them customer base
Fraud	A form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name.	A hacker steals people's personally identifiable information resulting in identity theft by using that individual's information to make purchases/makes changes to their bank account etc.
Destruction of Property	Attack results in damage or destruction of physical hardware	Any instance where the data theft or physical theft affects the physical properties of the equipment which the information was stored.

[32] https://www.surfwatchlabs.com/threat-categories#Target

Vandalism	The act of editing a website in a malicious manner that is intentionally disruptive. Vandalism includes the addition, removal, or other modification of the text or other material that is either humorous, nonsensical, offensive, humiliating, or otherwise degrading nature.	Website defacement is the most common form of web vandalism. This will often occur by hackers defacing a website with a photo and a socio-political message of some sort, usually attributing the attack to themselves
Service Interruption	Attack results in a service or website to be unavailable for a period of time. Often times this is a result of a DDoS attack or after a website defacement has interrupted the sites serviceability.	The Anonymous Hacktivists deface websites of the US government with a message/photos etc. This takes over the web site, not allowing customers/internet users to access the site – interrupting the service.
Infected/Exploited Assets	A computer or server or network has the potential to, is currently, or has been infected or exploited.	When a hacker infects a mobile phone through an application and can make changes to the device or infect it with mobile malware.
Device Hijack	A process through which a device has been taken control of by another user.	Hijacked webcam, remotely activate lights
Security Bypass	Vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of an application or system.	Security tools compromised, security breached, Facebook security breach

APPENDIX C - Spectrum for Cyber Defense

Another model includes a larger spectrum of cyber defense options, including elements that might be included in a campaign plan organized and led by the US Government.

Impose Consequences – the away fight

- All instruments of power – far more than cyber

Active Defense – the local, close in, defense

- Active engagement of adversaries with "limited pursuit"
- Proportional response to staunch an ongoing event
- Public and private sector roles defined to complement

Establish Vigilance and Cognizance as a basis for action

- Within the authorities and physical/virtual limits of a given system

- Vigorous, comprehensive & shared intelligence (local, commercial, government)
- Continually assess readiness and take action(s) to redress
- Red team and hunt within owned networks - presuming breach
- Conduct disaster exercises, Continuity of Operation exercises
- Establish thresholds requiring action and implement them

Establish Inherent Resilience – *through voluntary, incentivized or compelled means*

- Analogous to traditional Information Assurance
- Establish/leverage technology, doctrine, and procedures that yield defensible architectures
- Establish norms, and accountability (roles) for creating and operating defensible architectures
- Encourage diverse use of technologies to counter adversaries use of generalized tools that target common enterprise solutions

Define/Declare Priorities

- Define and prioritize the assets, capabilities, and conditions the organization is prepared to defend in and through cyberspace
- Private assessments (kept private) yield internal clarity, coherence and focus in business strategy and its IT components
- Public assessments (messaging) yields deterrence in adversaries and confidence in partners
- The delta between public and private yields uncertainty for the adversary and maneuver advantage for system managers
- Aggregation of data creates higher risk, particularly with migration of social media and cloud services where multiple data stores are physically and/or logically co-located

Planning

- Define business (organizational) objectives and determine their dependence on information technology, networked systems, processes, and data sources
- Tailor the components of defense and deterrence to deter extant (known threats), anticipated (projected threats), and prospective actors (vulnerabilities)

The table below highlights the aforementioned options and includes where attribution is required because the consequence of the defensive action has a direct impact on the source of the attack. Each category has an effect, in some cases it imposes direct cost on the adversary; in others, it denies benefits as vulnerabilities are closed.

Active Cyber Defense

Introduction

"Active defense" is a contentious topic in the cybersecurity debate in the United States. The term itself has become associated with vigilantism, hacking back, and cyber privateers, threatening to create a destabilizing global free-for-all between private actors in cyberspace. Even if the US were to authorize companies to take limited measures against cyber adversaries, these actions would remain illegal under foreign laws, and expose US companies to legal action if they took action on foreign networks. Taking action against an adversary can also antagonize the attacker and cause them to escalate. But a compromise position is possible, one that allows some increased leeway for companies to protect themselves, while limiting the dangerous side-effects of sanctioned private tit-for-tat cyber battles across international borders.

Policy Proposal

The federal government should explore options to empower private companies to engage in limited active defense measures, provided that these activities are carried out with prior approval and oversight from law enforcement and conducted exclusively on networks under US jurisdiction. This is different than hacking back. Under this proposal, taking unilateral retaliatory actions against an adversary's or third party's infrastructure or targeting other data on those servers would remain illegal. Any action on infrastructure outside the US, whether it belongs to the attacker or to third parties, would also be out of bounds, as this would violate international law and could destabilize US international relations. To protect innocent third parties and to prevent vigilante justices, it is imperative that any measure taken by private companies are consistent with U.S law and coordinated and authorized with law enforcement agencies (most likely requiring a warrant to enter a third party network) in advance.

This proposal has some important advantages. First, it could help to address companies' frustration at the seeming impunity of malicious cyber actors and lack of capacity of the government. More importantly, it allows companies to take some limited actions to mitigate cyber attacks, helping to reduce the burden on law enforcement and the government to defend private networks in the US. If companies are able to recover or delete data stolen from their networks before it reaches the adversary, they can prevent damage to and protect consumers, and take away the attacker's incentive to try to steal data from US networks. If the data has been deleted from the victim's network, this could also allow them to recover more quickly. Furthermore, the act of tracking down and recovering data from attacks could generate valuable evidence that could help lead law enforcement to the attackers. Finally, this could help streamline and expand existing efforts to take down attack infrastructure like botnets and malicious hosts, where the private sector holds essential access and expertise.

The proposal also has drawbacks, however. It may not be very effective, as stolen data is often transferred to a variety of third party servers in multiple countries almost instantaneously, making it difficult or impossible to keep the data from falling into the adversary's hands, and to have confidence that the data has been retrieved or deleted. Going through the process of working with law enforcement to get approval also means that defenders would remain slower and less agile than attackers. Taking down attack infrastructure could also have limited value, as compromising hosts and establishing malicious domains is a cheap and widely available service on the hacker black market.

It would also be difficult in practice for companies to limit their activities to US networks. It may not be obvious to the victim where the infrastructure storing their data or attacking their networks is actually located, or who owns it. Furthermore, this could lead to companies inadvertently damaging third party infrastructure or compromising other data on the targeted servers. Most importantly, while this might help contain damage to victims from cyber attacks, it would not raise the cost to attackers in a way that would deter future cyber attacks on US companies.

Zero Vulnerabilities

As our world grows increasingly reliant on computer systems and networked infrastructure, the risk that software vulnerabilities pose to critical information systems has grown dramatically. In many respects, software vulnerabilities have become commodities; they are traded on the market, offering opportunities for the highest bidder to gain unauthorized access to critical systems. Exacerbating the issue, many of these critical systems use components that are comprised of open source software - code which is not owned by any one responsible vendor or party - and thus often go unmaintained or under maintained, creating situations in which vulnerabilities may go unnoticed and unpatched for years.

The exchange of information about vulnerabilities has grown into a complex and sometimes illicit marketplace. This reliance on the market to fix insecure software has led to an arrangement in which vulnerabilities are neglected, jeopardizing both the companies that use the code and the infrastructure that runs on it. Modern software companies are faced with unbalanced incentives as they go through the challenge of searching for vulnerabilities not just to improve the security of their own products, but also ultimately to support national security.

Today, one of our most promising efforts to patch vulnerabilities in critical software has been incentive programs for security researchers to find and fix bugs. These so called "bug bounty" programs, in which companies pay researchers in exchange for information about vulnerabilities, have become a key tool to secure the infrastructure we all use.

However, there remains great legal uncertainty about whether or not security research is lawful under the current legal regime. Researchers fear that they could be prosecuted under the Computer Fraud and Abuse Act (CFAA) or for violating often arcane End User License Agreements (EULAs) even if their goal is to help secure an insecure system. There are also a number of collective action problems that keep researchers and companies from focusing on the most important categories of software.

Current efforts up to this point include industry specific vulnerability disclosure processes as in the Industry Control Systems Computer Emergency Response Team (ICS-CERT) guidance. Bug bounties for individual government websites such as the discontinued "Hack the Pentagon" program. And the vaguely defined Vulnerability Equities Process (VEP) that governs vulnerabilities discovered by select agencies.

The lack of a consistent regime for conducting vulnerability research and disclosure is hindering efforts to find and fix critical vulnerabilities. Lack of agreement of what constitutes legitimate security research increases costs for researchers. In light of this uncertainty, market incentives are insufficient to maintain the safety of core internet infrastructure, and inconsistent vulnerability release processes within government weaken strong norms around responsible vulnerability research and leave US markets vulnerable to cyber intrusions.

The US government and the private sector need to come together to establish responsible vulnerability research and disclosure processes, eliminate legal risk, and fund efforts to secure the internet. The US government can lead the way and establish norms around finding and fixing vulnerabilities by publicly committing to the same vulnerability disclosure process that it encourages the private sector to adopt.

Recommendations

In recognition of the risks to US economic national security posed by unmitigated critical software vulnerabilities, the Task Force makes the following recommendations:

- The President should clarify the legal status of vulnerability research by working with the security research and software engineering communities to publish a "code of conduct" for cybersecurity researchers that describes appropriate processes for reporting vulnerabilities found in corporate software as well as national infrastructure. Adherence to the code should provide legal safe harbor for researchers and support the growing security research industry that works to safely incentivize the detection, reporting, and mitigation of critical vulnerabilities. To develop this code, the government should specifically engage in a public-private partnership with the security research and software engineering communities to gather best practices on vulnerability reporting, building on existing efforts such as the National Telecommunications and Information Administration's multi stakeholder vulnerability disclosure process. The President should convene key US stakeholders and incentivize them to publicly commit to adopt the code of conduct by the end of 2017. Incentives should include preference in US Government procurement competitions and services contracts. To effect the safe harbor protections, the President should propose practical legislative language to Congressional leadership and consider bundling legislation with other national security-related bills for passage by the end of 2017. The Task Force notes this type of legislation should be a relatively strong candidate for bipartisan support, given the significant benefits to national security and commercial interests. To update the President personally on progress, two nationally known security researchers should be appointed to the President's National Security Telecommunications Advisory Committee and the President's Council of Advisors on Science and Technology by July 2017

- The President should encourage responsible vulnerability disclosure by directing the Department of Commerce to spend $100M per year to fund existing programs for securing common Internet infrastructure. Given the increasing significance of open source software in internet infrastructure this funding should prioritize ensuring that open source software is secure and sustainable. Independent, respected programs like the Linux Foundation Core Infrastructure Initiative, which provides financial support to critical Open Source infrastructure projects and The Internet Bug Bounty, which rewards persons for finding and fixing vulnerabilities in open source projects should be directly funded by the US government, but should remain largely independent. The President should also direct the Department to Commerce to create a government-run bug bounty and remediation program, funded with another $50M per year, specifically in support of open source projects that are widely used in government and commercial critical infrastructure, to fill gaps in the existing array of bug bounty programs and focus on work that would improve US national and economic security. The Task Force applauds the initial steps the Department of Defense has taken to create a bug bounty program for its own non-critical software and encourages the program's expansion. The abovementioned $150M per year of new funding should be transferred by the President's Office of Management and Budget from underperforming Federal Government cyber defense programs or from

classified cyber offense programs that increase the risk of a foreign counterattack on US critical infrastructure. The Task Force notes that this level of US government funding may not be suitable as a long-term component of sustainable open source security, but is critically needed today to catalyze broader investment and support.

- The President should expand existing Federal efforts to disclose vulnerabilities in critical infrastructure, such as the Department of Homeland Security's ICS-CERT vulnerability disclosure process, and mandate via an Executive Order that all Federal agencies must publish all security assessments of unmodified open-source code. Previously unknown vulnerabilities in all other software should be reported to vendors in a timely manner according to the previously described code of conduct, and the reporting timelines should be recorded and published. As an upper limit, any unclassified vulnerability discovered by or for the US Government should be published one year after its discovery, and unclassified security assessments should be published within 90 days of the evaluation's completion.

Baseline Security

We live in a highly digitized world, where our economic system, critical infrastructure, and social lives are increasingly interconnected, machine-to-machine. In fact, a study by Juniper Research estimates that by 2020 the number of connected devices will be over 38 billion. This growing interconnection is creating new business opportunities and value, but is also introducing new risks. Many systems are not designed to operate in a manner to mitigate these risks and as such there must by efforts taken to establish broad baseline security and mitigate risk across a wide array of different infrastructures.

In working to develop collective solutions to what has become a challenge to the common reliance on our digital infrastructure, all organizations, no matter the size, have an obligation to strengthen their baseline level of cybersecurity knowledge, understanding, and best practices. They must do this not only to better secure their business and data of their customers, but for the sake of our interconnected digital society itself and the security of the broader digital ecosystem. While most organizations acknowledge the need for collective solutions to this challenge, many still struggle with the persistence and growing sophistication of cyber threats. Cyber risk is difficult to accurately quantify, understand, and mitigate, and the realization that they must address this risk largely on their own often leads to inaction.

In its 2008 report, "Securing Cyberspace for the 44th Presidency,"[33] CSIS tackled the issue of baseline cybersecurity hygiene in depth. In the report's recommendations, the Commission called on the government to rebuild the public-private on cybersecurity to focus on key infrastructure and coordinated preventative and responsive activities. The report also sought to balance cooperation with regulation, acknowledging that market forces alone could not incentivize the level of investment needed to raise the bar for organizations facing national defense-level threats.

Since 2008, significant progress has been made in developing public-private partnerships. Through industry engagement efforts such the National Security Telecom Advisory Committee, information sharing legislation, and the work of the Department of Homeland Security and the Department of Commerce, the government is increasingly able direct its funding and knowledge towards raising the bar for security of private entities.

One of the most high-profile examples of this was the 2014 Cybersecurity Framework, developed in a partnership between the Federal Government and engaged members of the private sector. The Framework relates common cybersecurity risks with basic controls and organizational processes in order to empower organizations to protect their own systems and data, as well as their customers. Organizations are already using the Framework to design modern cybersecurity programs customized to their unique business environments, and this continues to provide a successful mechanism for evolving best practices around cyber risk management. Another area of partnership that has grown since the Commission's first report is in the realm of information sharing. The passage of the 2015 Cybersecurity Information Sharing and Analysis Act, after years of work by government and private sector policy experts, enshrined in law liability protections for corporations sharing cyber threat information, and developed a channel for alerting the private sector to threats known by the government, all while working to strike a balance that would have security

[33] https://csisprod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf

supporting privacy. While imperfect, the legislation stands alongside efforts to better organize like-minded corporations into Information Sharing and Analysis Organizations[34] and other private sector led information sharing groups.[35] However, moving beyond the recent focus on sharing of technical cybersecurity indicators, the time is right for organizations to share more information on the efficacy of defensive strategies and tools.

Technology solutions have a short shelf life. What maybe a good solution today may not be a good solution tomorrow. Enhanced sharing of the effectiveness of security technologies and configurations is a key step to advancing cybersecurity and understanding when solutions are becoming ineffective. As new security products emerge and companies grow, facilitating this dialogue would allow organizations to evaluate technologies far more quickly and enable better resource planning by security teams.

Another area that shows value in making organizations more efficient and effective in their security practices is the growth of third party security services. In many cases, the handling of data isn't an organization's core business or competency. For these organizations, data management distracts from their core business offerings and can lead to data breach due to underinvestment. This problem is exacerbated as a result of too few qualified security personnel, challenging many organizations to properly protect their infrastructure. Third-party security services should play a larger role in filling gaps that exist in many enterprises today. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization. In particular, cloud services offer significant security benefits, with lower cost and higher effectiveness than the average enterprise with self-managed IT. Beyond technical solutions, one area that has grown in focus is the increased attention given to making better strategic investments in risk management from corporations' boards of directors.

Corporate boards of directors are increasingly taking on the responsibility to ensure that their companies are taking appropriate steps to minimize cyber risks to their organizations and customers. A 2012 governance survey by Carnegie Mellon CyLab concluded that "boards are not actively addressing cyber risk management," finding that only 25 percent of the study's respondents (drawn from Forbes Global 2000 companies) reviewed and approved top-level policies on privacy and cybersecurity risk on a regular basis.[36] When the same survey was run again in 2015 by Georgia Tech, the findings showed a dramatic increase in board level attention, with over 63% of respondents stating that they actively address cybersecurity in the boardroom.[37] These figures indicate strong and growing support among boards to be more proactive in overseeing cybersecurity risk management.

While regulation has been slow to materialize, incentives and requirements for better cybersecurity have begun to grow from existing market forces, such as the developing

[34] https://www.dhs.gov/isao
[35] http://cyberthreatalliance.org/
[36] http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf
[37] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/governance-of-cybersecurity

cybersecurity insurance market,[38] and regulatory guidance, such as the SEC's work informing investors on corporations' cyber risk.[39] Along with providing more transparency for investors on cyber risks, the security community can support the removal of the stigma of disclosing information pertaining to damaging cyber incidents.

There is a need for companies to disclose what occurred, disclose what was lost, and share lessons learned with their broader industry. Instead of developing commercial competitive advantage through stovepiped, confidential efforts to improve security, the Government and commercial security community must work together to improve security of all connected organizations. This view is similar to the philosophy of the National Transportation Safety Board (NTSB), which investigates transportation accidents, discloses findings in a proactive and productive way, and issues recommendations to improve transportation as a public good.

The CSIS Task Force believes that all organizations should begin with a focus on baseline security so they can (1) assess their own risk and compare it against their peers, especially similar-size organizations in the same business sector; (2) determine whether they are investing appropriately given their risk tolerance and dynamic threat environment; and (3) work together to collectively make improvements that will benefit organizations across sectors. The recommendations in this section call for not just an increase in accountability, but also in transparency.

We, as security professionals, believe that organizations can work together to share experiences with security technologies, lessons learned from breaches, and look for opportunities to outsource tactical security operations so that organizations can focus on strategic risks. The recommendations detailed below are based on the premise that strong baseline security should be in the common interest of all organizations -- even competing companies -- and security professionals should work together whenever possible to make a material impact on our collective security.

In recognition of the critical importance of improving organization's baseline security, the Task Force makes the following recommendations:

Organizational Governance

The Task Force makes the following recommendation to further increase board oversight of cyber risk:

- To support stronger governance of cyber risks, the President should direct the Department of Commerce and request the Securities and Exchange Commission (SEC) to educate directors and senior executives about cybersecurity risk management best practices and corporate oversight responsibilities. Public company boards should also be required to incorporate cybersecurity into their existing corporate risk management efforts, building on the SEC's existing guidance to require public disclosure of material cyber risks, and to establish processes for regularly assessing and auditing this risk in a

[38] https://www.dhs.gov/cybersecurity-insurance

[39] https://www.sec.gov/spotlight/cybersecurity.shtml

common format that enables comparison among different companies. To support these activities, boards should be encouraged to retain cybersecurity advisory capacity either among their own members or from independent external consultants.

- To encourage the growing cybersecurity insurance marketplace, the President should continue to support the efforts by the Department of Homeland Security to incentivize and study this area. This study should also include a focus on externality costs from damages associated with a catastrophic event to critical infrastructure. Corporations should also work to better understand the effectiveness of technical cybersecurity investments so that strategic decisions can be made in order to appropriately mitigate cybersecurity risks.

Basic Security Hygiene Standards

The Task Force makes the following recommendation to further increase the adoption of basic cybersecurity hygiene standards:

- To support broader adoption of cybersecurity standards and best practices, the President should continue to incentivize implementation of the Cybersecurity Framework. Sector specific agencies, industry groups, and individual organizations should all work to adopt the Cybersecurity Framework to their individual sector or circumstance, so that common baselines are established for basic cyber hygiene. Work done by the prior Administration on incentives to implement the Cybersecurity Framework should be continued, with specific attention paid to cybersecurity insurance, liability limitation, streamlined regulations, tax incentives, and rate recovery. The Department of Commerce should present a progress report on these incentives and Framework adoption to the President every quarter. Existing cybersecurity regulations from sector specific agencies should be streamlined with the risk-based approach outlined in the Cybersecurity Framework. All US Government cybersecurity initiatives and publications should use the common terminology in the Framework. As the Cybersecurity Framework grows in adoption, the US Government should evaluate it annually and seek to expand its relevance for specific sectors.

Solution Lifecycle/Technology Advancements

The Task Force recommends the President should expand the 2015 Cybersecurity Information Sharing Act to include sharing information regarding the efficacy of third-party security models including the minimum standard of care for data security, methods for securing that data, and processes for recovering from breaches. Specific recommendations for each of these areas follow below:

- **Technology Lifespan** - The Task Force recommends the President should direct Federal agencies to reevaluate their use of software that has exceeded a ten-year lifespan. Systems that have exceeded this timespan, and are not considered mission critical, should be replaced and any savings in program funding should be applied towards strengthening the cybersecurity efforts at the agency.

- **User authentication** - The Task Force recommends sharing information on new technologies and best practices that reduce the reliance on passwords for user authentication. The President should require the Federal Government to lead by

example and move away from passwords and to multi factor identification, annual audits for password processing systems, login anomaly detection systems, server side analytics, increased awareness of and education about secure authentication practices, and the wider adoption of HTTPS. Any Government system that still relies on single-factor authentication or lacks HTTPS on January 1, 2018, shall be a candidate for shutdown, with its funding reallocated to other Presidentially directed cybersecurity initiatives.

- **Full Asset Coverage** - The President should issue an Executive Order that directs OMB, in conjunction with Department and Agency leadership teams, to prepare a plan for securing all IT assets, including all IoT devices, smartphones, tablets, printers, and other network-connected devices for the President's approval no later than 60 days after assuming office. The plan should include specific, actionable steps that every agency will take to implement the plan, including their associated costs, no later than 60 days after Presidential approval of the plan. OMB and agency heads will review and assess implementation progress as a key metric to guide Department and Agency budgetary development for FY2019.

- **Cloud services** - The Task Force recommends cloud service providers should describe their best practices for security and provide results of audits and self-assessments against these best practices. The President should also provide procurement preference to providers that follow these practices.

Disclosure of Cyber Incidents

The Task Force recommends the President and Congress create an anonymous clearinghouse for mandatory cyber post-incident reporting that would offer limited liability protection for participating entities:[40]

- This clearinghouse would be housed within the DHS National Cybersecurity and Communications Integration Center, and include representatives of industry ISACs to facilitate communications. Anonymized assessments, including pen test results, should be made available through this clearinghouse including technical data on known breaches, and prioritized lists of best practices and effective controls tied to the Cybersecurity Framework.[41] To affect the liability protections, the President should propose practical legislative language to the Congressional leadership and consider bundling it with other national security-related bills for passage by the end of 2017.

[40] To enable this disclosure, organizations would need to be granted a level of immunity for reporting any breach within 30 days of discovery and the role of law enforcement would need to be considered carefully. Steps should also be taken to ensure that disclosure does not educate an adversary on defensive measures being taken to stop an attack in progress.

[41] Information that would be beneficial to learn from the reporting includes;

- What security policies, tools, and governance did an enterprise have in place?
- What was the overall IT architecture and when was the system last tested, and for what?
- How was access governed?
- What was the source of the breach, how was it detected, and what was taken?

Data Protection

Data is the currency of value for attackers; cyber intrusions are simply methods to obtain it. Protecting this data is paramount. A focus on merely preventing intrusions or only protecting small classes of data is insufficient to protect consumers and businesses. There are many ways data can be abused, and adversaries are motivated to obtain a far broader range of data than what is effectively protected.

Organizations often do not fully understand the value of the data they hold and fail to take appropriate steps to protect it. For example, in 2006 an online movie distributor released an "anonymized" data sample set as part of a research contest – however, security researchers were able to de-anonymize the data to reveal many individual movie preferences, some of which were indicative of personal private preferences and beliefs. The recent OPM data breach of Federal Government employee background checks reveals the perils of losing Personally Identifiable Information (PII) that in the wrong hands could have devastating consequences, well beyond financial or identity theft.

Data outside the traditional PII classification, especially in aggregate, has sensitivities that have not been accounted for. Online data is expected to grow significantly year over year in the next decade. This data predominantly falls outside current protective PII and healthcare protection frameworks, yet is increasingly revealing of our day to day lives. More than just online activities, data is a diverse representation of both our online and physical world. Consider the intimate portrait painted by a user's location tracking, detailed health statistics, personal shopping preferences, beliefs, social associations, and financial status. Most individuals would consider this data to be private information, yet it currently receives no legal protection.

New types of private data are also cropping up every day. The rapid proliferation of location tracking technologies illustrates how quickly new data types and uses can develop. Few of us would have predicted 10 years ago that we would each carry devices not only with the ability to track our every movement but also share real time location data with others around the world.

Current business practices around amassing privacy sensitive data presents a classic negative externality. The costs associated with a privacy breach are unduly borne by society and the individual. Without economic incentive to apply controls or least privilege, current business practices are drawing criticism domestically and abroad.

There are several previous and ongoing efforts to protect personal data: The White House's proposal of a U.S. Consumer Data Privacy Framework which proposes a multi-stakeholder process for defining a baseline code of conduct and expanding enforcement authority beyond the FTC to include state Attorney Generals; the recently finalized E.U.-U.S. Privacy Shield which offers new international redress mechanisms if companies do not comply with their own privacy policies; and the FTC's ongoing efforts to enforce existing privacy policies under section 5 of the FTC act which bars unfair and deceptive acts and practices in or affecting commerce.

These efforts represent significant progress, but do not go far enough or have not been acted

upon. For the most part, they rely upon the enforcement of existing privacy policies which to date do not describe protections for data and suffer from the critiques above. With an increased global focus on data protection, more work is needed in the US to clarify the value of personal data and measures that can be (or are being) taken to protect it.

Similarly to efforts already underway to increase cybersecurity, there must be a renewed focus on education and strengthening data security. This recommendation provides protection to all kinds of consumer data and offers a flexible framework for companies to self-describe the data protections they provide. Market forces, consumers, and insurance agencies can use this to reward companies providing proper data protection. It also opens up enforcement possibilities for companies that do not uphold their data protection guarantees. Lastly, unlike a static legislative framework, this allows companies to adjust their data protection strategies as new types of data and data protection technologies become available.

A key enabler for these recommendations is passage of national data breach legislation that meets the highest current requirements and unifies the dozens of state laws in a single national standard. This would focus corporate data protection efforts on a single, well-understood regime; and provide a long-awaited legislative vehicle for other major reforms listed below.

Recommendations

In recognition of the critical importance of this data and its protection, the Task Force makes the following recommendations:

- The President should promote and encourage good data security practices by directing NIST to develop a set of recommended Data Security Standards and Practices that are updated annually. This should include guidance on what data types should be considered sensitive and what data is currently regulated, as part of the effort to broaden the definition of personal data beyond the current legal definition of PII, and to help establish generally acceptable standards or care for that data. This document should be described in plain English and use iconography that is easy to understand – perhaps borrowing inspiration from nutritional facts labels on foods. It should also utilize the terminology of the Cybersecurity Framework, if possible, and draw on anonymized lessons learned from past cyber incidents, including input from a wide range of Corporate Data Security Officers, and be endorsed by both civilian (e.g., Department of Commerce) and national security (e.g., Department of Defense) parts of Government. The first version of this document should be published by the end of 2017, with a Presidential foreword explaining the value to US consumers, business leaders, and investors.
- The President should encourage the voluntary publishing of annually reviewed Corporate Data Security Policies for public and private entities that collect personal data (including traditional PII and the broader range of potentially private data described above). The policy should describe the kinds of data that will be collected, the expected uses for each kind of data, the entities the data is expected to be shared with, and how long the data will be retained. The policy should also describe the mechanisms employed to protect the data from unauthorized use and loss. The President should publicly laud companies that publish their policies, via a major event

held at least once per year (perhaps a larger version of President Obama's 2015 cybersecurity summit at Stanford University), and emphasize the value of this transparency to US consumers, business leaders, and investors.

- The President and Congress should require all major organizations in the US that hold sensitive data (as defined by NIST) to appoint Corporate Data Security Officers, to help protect those organizations, US employees and consumers, and US national and economic security. These officers would develop Corporate Data Security policies and standards, educate employees responsible for handling data, ensure companies conform to their self-stated policies and practices, and ensure that company officers are informed regularly of company data security practices & risks. A taxonomy of privacy relevant data types should be developed along with some potentially non-linear cost multiplier against the number of records involved. This regime should also encourage information sharing, and be made available to support a healthy cyber insurance market. These officers would also be the primary contacts for all US Government cybersecurity initiatives. This role may be given to an existing Chief Security Officer or Chief Privacy Officer, if those roles already exist. To promote appointment of these officers, the Cabinet departments and General Services Administration must require organizations to name their Corporate Data Security Officers by the end of 2017, in order to receive any Government contract, funding, or data, or to operate any part of US critical infrastructure.

- Corporate boards should be encouraged to review their company's cybersecurity preparedness with their Corporate Data Security Officers at least annually, and this review should feed into Securities and Exchange Commission requirements for public companies to disclose cyber risk.

- The President should request the Federal Trade Commission (FTC) to create a Division of Data Protection, staffed with technical experts in addition to law and policy experts, to provide consumer-facing education, publish an annual assessment on the quality of consumer related data protection, and act as an advocate for consumers in matters of data protection and security. This Office could create a recognized seal or Better Business Bureau-style rating system that recognizes and promotes good data protection policies and behavior, as a way to encourage major companies to better protect consumers and avoid costly and embarrassing FTC sanctions.

Workforce Acceleration

A continually cited barrier to improving the U.S.'s ability to tackle difficult cybersecurity challenges is the lack of qualified personnel with the proper combination of technical skills. Among the authors of this Task Force, there was broad agreement that hiring of well-trained cybersecurity candidates was growing increasingly difficult due to skyrocketing demand. Anecdotally, many shared the same experience, that they would either be forced to hire inexperienced candidates they could afford and then risk losing them to higher paying positions soon after they were trained by a company, or to be that company looking to pay huge sums to steal experienced candidates away from their current jobs. Clearly, demand for diverse and qualified cybersecurity professionals continues to vastly outstrip supply and recent studies provide some hard evidence to back these observations.

A recent report from Stanford University noted that as of March 2015, more than 209,000 cybersecurity job positions remained unfilled and postings for these positions have grown by 74% over the previous five years.[42] Cisco has estimated that the shortfall of IT security professionals worldwide is over 1 million jobs,[43] and a recent 451 Research study found that two of the greatest challenges for improving security in large organizations are cybersecurity expertise and inadequate availability of qualified professionals.[44] In addition to the impact to the private sector, of low availability of qualified personnel, the Department of Defense has consistently noted for years the importance of growing the cybersecurity workforce for our national defense. In its 2013 Cyberspace Workforce Strategy the Department stated that, "There is a recognized pervasive national shortage of skilled cyberspace personnel, potentially impacting the operational readiness across the Department and putting national security at risk."

In 2010, CSIS helped raise the focus on this issue through its report, A Human Capital Crisis in Cybersecurity noting that, "The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government."[45] The landscape at this time was significantly more challenging that today due to a lack of accredited training opportunities and a strong debate over the value of professional IT certifications. The report described the cybersecurity profession to, "19th century medicine – a growing field dealing with real threats with lots of self-taught practitioners only some of whom know what they are doing."

Since that time, the U.S. Government has prioritized efforts to address this national gap in standardized training and professional development through the National Initiative for Cybersecurity Education (NICE) program which coordinates Federal policy and agency efforts to engage the education community. The President recently requested $62 million from Congress to Expand Scholarship for Service, develop a Cybersecurity Core Curriculum, and support the National Center for Academic Excellence in Cybersecurity program. The President also announced that the Government will work to enhance student loan forgiveness for cybersecurity experts joining Federal employment and add cybersecurity to the President's Computer Science for All Initiative.[46]

While there are steps being taken to close our cyber skills gap, we have to ensure these efforts

[42] http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/
[43] http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf
[44] https://451research.com/voice-of-the-enterprise-vote-information-security
[45] https://www.csis.org/analysis/human-capital-crisis-cybersecurity
[46] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

and more are carried forward to establish cybersecurity as a fundamental subject of learning in the U.S. educational system. Along with the long term growth of our national cyber workforce pipeline, the Task Force also believes that we are leaving out strong pools of talent available in the immediate term by not fully tapping into veterans' communities and retooling immigration policies to take better advantage of highly skilled individuals coming into our country. Solving the human capital shortfall is critical to our national cybersecurity posture and as such this Task Force recommends policy action by the next President across three areas: Cybersecurity Awareness, Education and Training, and Legal Reform.

In recognition of the critical importance of accelerating the growth of our cyber workforce, the Task Force makes the following recommendations:

Increased Funding for Cybersecurity Education, Training, & Awareness

The Government has made progress on raising funding levels for cybersecurity education, training, and awareness among the US public, however, currently proposed funding levels are inadequate given the importance of driving a larger cyber workforce pipeline and increasing training as well as general adoption of cyber hygiene best practices.

- The Task Force Recommends that the President direct key departments to re-allocate additional funding to support cybersecurity education, training, and public awareness programs, to $100M per year. This should include continued support for existing programs and organizations such as the NICE, Scholarship for Service, National Cyber Security Alliance, and support for new programs funded through the Department of Commerce. These programs should also seek to engage minority candidates that are not typically represented in STEM programs. Furthermore, private industry should be encouraged to match Federal Government spending levels with $100M of their own funding, due to their interest in solving workforce issues for their own benefit. The President should convene private sector leaders, gather funding commitments, and launch the new $200M (combined Government with private sector matching funds) program as a single landmark initiative before the end of 2017.

Education and Training

Cybersecurity education and training is at the heart of this Task Force's recommendations. Education across age and other demographics is crucial to upgrading our human capital for cyber professions, but engagement early at the elementary school level provides some of the greatest areas for growth. We recommend a range of education and training programs be implemented at the federal, state, and local levels. Growing the pipeline of qualified students in cyber is the only sustainable method to ensure our nation's continued cybersecurity. The Task Force recommends the Administration take the following steps across our education system.

Elementary & High School Level

Elementary and high school systems should establish mandatory, basic cybersecurity awareness curricula for all students, focusing on online risks as well as general IT knowledge. The goal of this initiative is for cybersecurity to become as widespread as traditional civics classes.

- The Task Force Recommends that along with the current Presidential initiatives, Federal and State funds should also be directed to support the availability of white-hat hacking courses, development of model curriculums, and competitions with a focus on making

security and IT skills more broadly accessible and relevant for young people. Finally, security should also be a core subject in computer science classes and security and cyber ethics should be included in advanced or honors level computer sciences courses. The President should present this vision to the National Governors Association to promote state and local funding of basic cyber security awareness programs, to help protect our nation's children and develop high-value career skills.

Collegiate & University Level

Similar to the high school level, security should be a core part of accredited computer science curricula in our nation's vocational schools, community colleges, and universities.

- The Task Force Recommends that the President and his Council of Advisors on Science & Technology, along with the Department of Education and National Science Foundation, should convene top US presidents, administrators, and accreditation organizations of higher education institutions to promote adding security to computer science curricula by the end of 2017, and emphasize this in every Government grant to universities. Higher education institutions, including US military academies and ROTC programs, should also support security research as a separate major, support and fund internships in security at government organizations and private corporations, and increase vocational training and apprenticeships at junior colleges and trade schools. The Federal Government should reinstate full STEM funding for college internships and research from organizations such as the National Security Agency and Department of Homeland Security with the goal of at least doubling the number of graduates by the end of the next president's term.[47]

Workforce Education

To support the development of better cyber hygiene in the workplace, organizations should promote general cyber security awareness programs among their employees. Online security training programs and certifications for non-IT professionals should be encouraged and taken into account by employers during the job promotion, search, and recruitment process.

- The Task Force recommends that the President should lead the way by helping recruit one Federal Government cybersecurity employee per year, with a personal phone call to close a high-value candidate to serve as an example.

Veterans

Veterans today are eligible for IT training programs, but more can be done to encourage the private sector to tap into this community for hiring qualified and vetted candidates.

- The Task Force recommends that the President should encourage technically inclined veterans to utilize GI Bill benefits for cyber specialized training programs in vocational schools, community colleges or universities, hold a major event at a Department of Veterans Affairs facility to promote this path by the end of 2017, and direct the Department of Defense to provide a quarterly update on veterans' training.

[47] Funding 500 internships annually would cost around $7.5m including overhead. The ROI on this recommendation would be high as it results in the direct identification, training, and recruitment of the next generation of our cyber workforce.

Veterans transitioning from cyber related military career fields are a unique resource. Not only are they practitioners in defending large networks, but they also have already undergone security clearance review. While private enterprises have clear demand for such talent, there is not a centralized repository for them to seek veterans.

- The Task Force recommends that the President establish a cyber-specific veterans job recruiting program to help bridge that gap. The expansion of existing programs should be first evaluated to prevent duplication. The Department of Defense should identify 100 willing Federal contractor companies that require security clearances and have job openings for cyber defense professionals, and launch a new two-year internship and recruiting program with this consortium and the Department of Veterans Affairs in a major event by the end of 2017.

Legal Reform

To fully encourage the growth of the cyber workforce, the next administration should enact several legal and regulatory reforms around security research and immigration policy.

Security Research

The uncertain legal atmosphere around security research and vulnerability disclosure policy has a chilling effect on the professional cybersecurity community. Legitimate research or participation in efforts to find and disclose vulnerabilities in software or services are often considered criminal offenses under current statutes, hampering educational exploration in computer security. Clarity in this area would help enable development of a creative, experienced, and empowered cybersecurity workforce.

- The Task Force recommends that the President should develop a code of conduct and legal protections for vulnerability disclosure and security research, as described in the "Zero Vulnerabilities" section of this report.

Immigration Policy:

While the aforementioned training and education underpins the future of our domestic cybersecurity workforce, increasingly, targeted immigration can be highly beneficial short-term tool to supplement our high-end cyber workforce. In addition, there are potentially strong national security benefits to drawing world-class cyber operations talent from other countries of interest to the United States.

- The Task Force recommends that the President work with Congress to establish a new visa category providing an allocation of 25,000 visas for foreign cybersecurity professionals or computer scientists to be employed at companies building cybersecurity products. This visa category would allow for fast tracking green card applications in order to ensure qualified individuals are able to remain in the country. The President should propose practical legislative language to the Congressional leadership and consider bundling it with other national security-related bills for passage by the end of 2017.