CHAPTER

15

Cyberspace Challenges

INFORMATION IN THIS CHAPTER

- Cybersecurity Issues Defined
- Interrelationship of Cybersecurity Challenges
- Way Ahead

This chapter is based on research conducted for a white paper developed by the company TASC under the CTO's office CyberAssure™ program. The study was designed to help customers understand the entire set of cyber challenges facing them today so they could determine where resources would best be used. It was done in conjunction with University of Virginia Applied Research Institute. The original authors were Steve Winterfeld, Anthony Gadient, Kent Schlussel, and Alfred Weaver. It is used here with their permission.

While updating this chapter, it has been somewhat discouraging that not much has been accomplished to change the disposition of these challenges. With the current state of the economy, there are not many funded research efforts going today so nobody should expect any dramatic improvements on the near term horizon.

Currently, the United States, Western Europe, and much of Asia have integrated the Internet into both their economy and military to the point they are dependent on it for daily operations. For the United States, these digital capabilities have become a strategic center of gravity. Additionally, most other nations are quickly moving in this direction. The number of systems (computers, mobile devices, infrastructure devices) and applications (stand alone, networked, and web-based) that support this cyber capability are growing exponentially. Due to this explosive growth, nations struggle with systems that are plagued with vulnerabilities that could easily impact our ability to maintain confidentiality, validate integrity, and ensure availability. This increasing reliance on technology has created significant national cybersecurity challenges.

At the same time, advanced technologies and tools for computer network operations have become widely available at low cost, resulting in a basic, but operationally significant, technical capability for U.S. adversaries of all types, including hackers (anyone conducting

Cyber Warfare, *Second Edition*
http://dx.doi.org/10.1016/B978-0-12-416672-1.00015-5

unauthorized activities on a system), insider threats hacktivists (cause-based hackers), industrial spies, organized crime, terrorists, and national governments (often called Advanced Persistent Threat or APT). In 2012 President Barack Obama said, "It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country" [1]. A comment echoed in his 2013 State of the Union address.

There is no single document that succinctly and comprehensively identifies the cyber challenges facing the United States and other nations, and then organizes these issues so that senior leaders can develop a comprehensive plan to address the challenges facing their organizations while the technical staff can identify which challenges most impact their organization. This chapter addresses this gap in three ways. First, it provides a concise review and taxonomy of the principal cyber challenges we face today. Next it lays out who should allocate resources to the different challenges. Finally it provides a look at the way ahead. It is not designed to provide the answers but rather to start a discussion about the next steps to prepare for success in cyberspace. While this chapter will focus on how the United States is impacted by these challenges they are uniform for all nations.

CYBERSECURITY ISSUES DEFINED

These challenges were selected based on customer feedback, Senior System Security Engineer input, and review of studies like: Institute for Information Infrastructure Protection's (I3P) National Cyber security R&D Challenges [2], Networking and Information Technology Research and Development's (NITRD) National Cyber Leap Year [3], InfoSec's Hard Problem List [4], Computing Research Association's Four Grand Challenges in Trustworthy Computing [5], Department of Energy's A scientific R&D approach to Cybersecurity [6], Center for Strategic and International Studies' (CSIS) Securing Cyberspace for 44th president report [7], Bush's National Cybersecurity Strategy [8], HSPD 54's Comprehensive National Cybersecurity Initiative (CNCI) focus areas [9], and Obama's Cyberspace Policy Review [10]. The authors picked the final list based on the major pain points they think our nation is facing. They acknowledge there are subjects that could be argued to be added, while some of the ones included are not applicable to every organization as well as they could be grouped differently.

The authors have categorized each challenge by level of complexity. The rankings are: Extremely Difficult (ED), Very Difficult (VD), Difficult (D), and Not Cost Effective (NCE). There is no clean way to rank them, as the types of resources are different for each challenge, so we have tried to quantify/qualify the complexity and types of resources needed. The term resources is not restricted to financial. In some cases it is classic research and development for new technology, for others it is political will, while others require new or changes to regulation. Some are dependent on external forces, others need financial investments and finally they all need some level of leadership focus.

We have also categorized the challenges by resources required, while we have stated that there are a number of types of resources this metric will focus on overall financial investment required. We have used the following designations to show the level of effort needed for each challenge: Very Significant = $$$, Significant = $$, Less Significant = $. While it is difficult to address how to categorize levels of resources, as different challenges require different methods to solve in general, we will use the initial unclassified CNCI budget of $18 billion as very significant, less than $9 billion as significant and less than $1 billion as less significant. These are very general estimates and each problem would need to be examined against a specific plan to determine resources required.

The challenges are grouped to show their relationships. The major areas are Policy, Technology, and People. The areas of overlap between them are Policy and Technology have process in common, Technology and People have skills in common, and People and Policy have organizations in common. Then there is a core set that is common to all the challenges (the mapping is shown in Figure 15.1). They are not listed by order of importance as each organization would rank these issues differently based on their risks.

This graphic has been used to lead workshops for all types or companies or organizations trying to determine where they should allocate resources based on which challenge is causing them the most pain balanced with where the level of investment they can make will have the greatest impact. The workshop starts with eliminating those challenges that are not appropriate for the organization (i.e., most companies do not have a need for Rules of Engagement policy). It then goes into discussion on what is critical for them. After a while the discussion usually comes down to should the organization invest in more technology (often monitoring focused) or in training (people focused). General agreement is that there is a desire to invest in changing the behavior of the users but the level of resources required to truly make an impact on how they act is not practical so most organizations default to buying tools to monitor them.

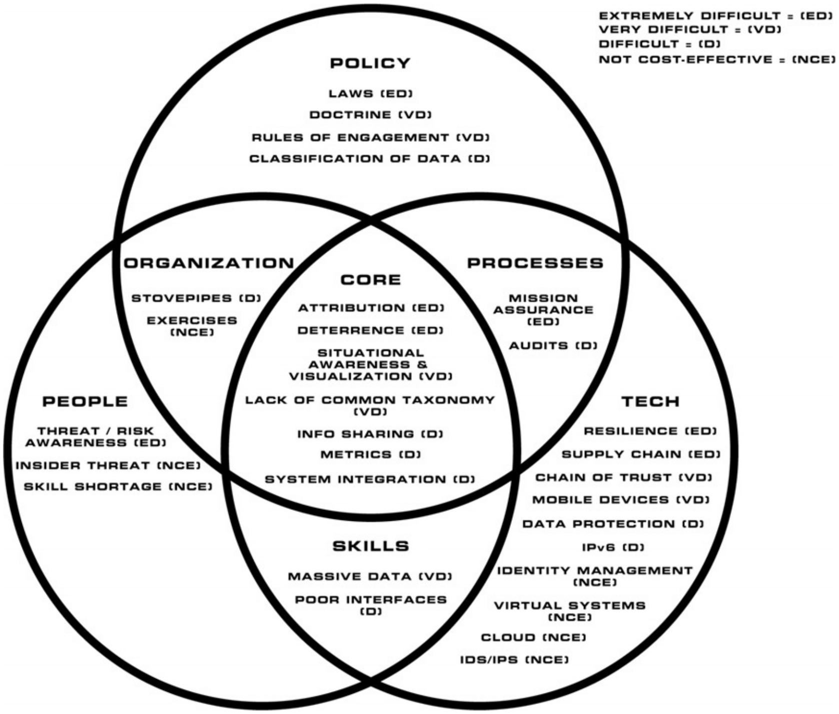

FIGURE 15.1 Categorization and relationships of the challenges.

Policy

Laws (ED $) encompass policy, legal issues, national security, and privacy. In the United States today, these issues tend to conflict with each other. Our culture and heritage influence the formation of our laws. Relatively speaking, cyber issues are new when compared to the backdrop of our legal system (dating from common English law and the Magna Carta in the year 1215). Our legal system lacks experience in setting boundaries for many of the technological advances today, to include cyber, medicine, and advances in communications. The legal issues are further complicated within the United States as each state sets its own laws that vary widely and even federal law is interpreted differently in various courts. There are a number of proposed regulations, statutes, and international agreements being worked today that will impact many of the issues discussed in this chapter.

Doctrine (VD $) suffers from a lack of consistency across the military services that address offense and defensive cyber strategy through tactics, techniques and procedures. This is not to say that there is a complete lack of doctrine or that it conflicts but rather there is no common unifying doctrine. The DoD has made progress by establishing a common set of terms [11]. Also each service has stood up commands and at the Joint level CYBERCOM has been stood up. Though much has been done the problem remains that there is no common vision of cyber operations and cyberspace warfighting doctrine.

Rules of Engagement (ROE) (VD $) are needed for local commanders who understand how to react to real world or kinetic attacks based on approved ROEs, but in cyberspace there is no common understanding of what constitutes a “use of force” or “act of war” on the Internet, hence, there is no agreed doctrine on how to fight a cyber war. If there is an attack, the response to the attacker (if attribution is accomplished) is not uniform. There need to be clear rules on what constitutes an incident or attack and what type of response (technical, legal, or diplomatic) should be conducted. One conundrum this challenge faces is where there is progress it is often classified.

Classification of data (D $$) issues is a result of each organization within the U.S. government utilizing different practices for classification of data, creating disconnects in the ability to work with non-DoD organizations. Even though there is one official set of rules, the implementation of the rules differs wildly among many agencies that handle classified documents. Coupling that with the different cultures in each organization, the sharing of data between agencies can often be difficult. Outside of the Intelligence Community (IC), the rest of the DoD and other non-IC agencies, people may not be able to discuss certain matters and properly collaborate due to lack of clearance. There is a move to increase the number of people with clearances but that will not address the issue as each crisis will require a unique set of experts to fix and there is no way to determine who will be needed beforehand. We need a system that can share information based on need, not background checks, while maintaining operational security.

Processes

Mission Assurance (ED $$) is the focus on protecting networks and information during operations. There is a need to fight through a contested cyber domain to make sure the operational tasks are accomplished to achieve the mission of the organization (this includes military systems, the Defense Industrial Base and the commercial backbone networks they use). What is needed is an understanding of which systems are critical to accomplishing the mission and how they can be used in a degraded mode (i.e., using a limited or alternate set of protocols) to continue to maintain maneuverability and basic capabilities in an environment that they may no longer control.

Audits (D $) are the regular, structured evaluation of an enterprise's IT systems, personnel, and processes. The audit process represents the measurement step in a continuous cybersecurity improvement program (implement ⇒ measure ⇒ correct). As such, regular cyber audits represent the keystone of any cybersecurity program. One key new collaborative resource is the "Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines" by the Center for Strategic and International Studies. These top 20 Controls were agreed upon by a powerful consortium including NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities [12].

NOTE

There are a number of complementary standards like Information Systems Audit and Control Association's (ISACA) Control Objectives for Information and related Technology (COBIT) or the International Organization for Standardization's Code of Practice for Information Security Management family of standards that can be very useful. These can be supported with processes like Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMI), and Six Sigma but there is no common industry-accepted practice today. Furthermore, today these audits are very manual and labor intensive; the trend needs to move to real time auditing via automation.

On a slightly different track we have the current set of Certification and Accreditation standards that are used today. The DOD Information Assurance Certification and Accreditation Process (DIACAP) and Director of Central Intelligence Directive (DCID) 6/3 processes as well as the Federal Information System Management Act (FISMA) process for all government agencies are undergoing change to be more focused on real-time monitoring. The NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations (Sept 2011) [13] is a great example of where they are headed.

Technical

Resilience (ED $$$) is designed to have systems self-heal with no intervention from humans. In the cyber context, a resilient IT system must continue to operate (as intended) even if compromised. For example, if unauthorized access is achieved. It should be noted that this is different than Continuation of Operations Planning (COOP), Disaster Recovery Planning (DRP) or reconstitution. Given the highly distributed nature of IT systems today, an important aspect of resilience is the ability of a system to meet its specified function in the face of denial of service attacks which might compromise network access. Resilience is therefore an attribute we need our IT systems to process. The challenge is to develop a resilient system, and in particular to design an enterprise-level system to be resilient in a contested cyber conflict environment. Rapid recovery in a contested environment will be key for military cyber conflicts.

Supply Chain (ED $$$) relates to the development and manufacturing of both hardware and software which has increasingly been accomplished in foreign countries. Traditionally, the military would build Government Off the Shelf (GOTS) software to meet their needs but today there is a trend to leverage Commercial Off the Shelf (COTS) and/or Open Source software to save costs. This problem is becoming ubiquitous. There is very little hardware or software that does not contain foreign components. With the increasing complexity of hardware, the verification and validation of hardware has become very difficult. If we can authenticate all the interactions among the hardware components in a system, then we can verify that the hardware does what it claims to do.

How authentication of hardware and software is done is the challenge. Many hardware components come from many different (and sometime competing) manufacturers and the software/firmware is integrated at different stages of manufacture. Every interface and transaction must be authenticated to insure the device works as advertised and that there are no hidden capabilities that can cause harm to the overall system or create covert channels and unknown vulnerabilities that can be exploited by advisories (be they nation state or criminal).

An example of the type of challenges that could arise from a supply chain attack is the intentional inclusion of a logic bomb in a hardware implementation by a potential adversary. This is of particular concern given the significant number of integrated circuits that are fabricated in Taiwan and China. I would like to lay out a complex attack that is a nightmare scenario. Imagine that a silicon chip includes circuitry whose existence is only known to a potential adversary. Imagine further that this silicon chip has been included in a variety of missile systems—air to air, air to ground, sea to air, and so on. Finally, imagine that a conflict arises with this potential adversary and the logic bomb is activated disabling the most advanced systems available to our forces and allies. Out of necessity, the conflict ends almost as soon as it begins and we have lost.

Chain of trust (VD $$) comes from the need for increasing trustworthy computing in an enterprise setting which can occur if we can authenticate all interactions among enterprise hardware supporting the enterprise users' computing needs. Such an approach using hardware that can authenticate every connection prevents or makes much more difficult a man-in-the-middle type of attack. An example would be when a command and control system sends an order to a weapons system: how does the sender know it was received, how does the receiver know it was really from the command and control system, and how do both know the contents of the message were not modified? In the commercial world this is done by digital signatures and hashing messages to produce a digest which will enable detection of any changes but these are not used in everyday system to system transactions and can be compromised if the root certification database is hacked.

Mobile devices (VD $$) are a challenge as more and more devices connect to the grid (i.e., smart phones, thumb drives, iPads, and laptops). There is a need to both protect them and validate their security before they connect. In many cases these devices are being used to conduct sensitive business and connected to protected networks with little to no security monitoring. The younger generation of workers are bringing their technology from home to the work place and doing work on their personal devices. They are connecting to more sites like social media which encourages sharing digital identity, postings about work, location services and photos. It is becoming a challenge for the security team to keep up to date with what is going on at the enterprise level of the network. One of the ways the security team can mitigate risk is to train the users on the risks involved. As mobile devices become more prevalent on the physical battlefield, this will become a key component of military cyberspace.

NOTE

DHS program—"Stop.Think.Connect" emphasizes four key cyber issues: Identity Theft, Fraud and Phishing, Cyber Bullying and Ethics, Cyber Predators. This program is a good resource when talking about safety on the internet [14].

Data Protection (D $) is the focus on providing the core concepts of information security "confidentiality, integrity, and availability" to the data rather than protecting the network or operating system layers. Today, in a fortress mentality, many organizations focus their cybersecurity efforts on protecting the cyber perimeter using products such as firewalls. This "line in the sand" or "Maginot Line" approach fails to recognize that a significant portion of the value of an organization's information system assets lies in the data that is stored on their IT systems. These data include more than just documents; it also includes emails, web pages, web apps, and key executables such as operating systems. One obstacle many organizations would need to face first is categorizing their data by level or importance/value. Therefore, a comprehensive cyber strategy should place significant emphasis on data protection in addition to any efforts that are applied to perimeter defense. When viewed in this information-centric manner, critical questions arise. We must ask if a perimeter defense is the most appropriate approach to data protection, or is an asymmetric, decentralized, defense required [15]. The answer is no and the solution is that we need to move to a new model. Many of the military weapons systems depend on the validity of the data they are using so this is crucial for accuracy.

TIP

When looking for process to use to implement security NIST has a very wide set of policies and guidelines: Guide to Enterprise Telework and Remote Access Security, Minimum Security Requirements for Federal Information and Information Systems, Guide to Security for Full Virtualization Technologies, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) are a sample of the dozens of resources available at their web site [16].

IPv6 (D $$) presents a challenge because during the transition to the new protocol there will be new opportunities for both defenders and attackers. In 2013 the Internet Corporation for Assigned Names and Numbers (ICANN) is predicted to be out of IPv4 Internet Protocol

(IP) addresses. This will force implementation of IPv6 over the next couple of years. Most of the challenge will come from upgrading equipment and finding staff with IPv6 skills. With the new protocol comes new security changes like so many addresses that scanning all the network addresses for an organization will become resource prohibitive which will cause a shift in tactics and tools. So while it is still early in the implementation phase, there is more security built into the protocol which means it will provide better security than today's version.

Identity Management (IDM) (NCE $$) consists of three functions that need to be accomplished when allowing personnel to access the network: authenticate—they are who they say they are; authorize—what they have access to; and audit—what they do. The days of IDM being just an 8-12 character password are dead. Today most companies are moving to tokens or biometrics to help ensure they are authenticating the individual (preferably using multiple factors). They are also building rules that limit what each individual can do so they only have access to what they need to do their jobs. Finally, auditing what they have done to validate policies are being followed. The issue is that there is no common standard today. There are efforts like the DHS which runs the National Strategy for Trusted Identities in Cyberspace program [17] that could help at the national level. Every fort or base has security around them to control access, it is just as important for the network they are using.

TIP

When dealing with a vendor selling cloud services it is important to understand there are three primary cloud-based delivery models. Be sure you are getting the right one for your organization.

- Software as a Service (SaaS): The user accesses applications that are on the network. This type of access has no effect on the user's local environment or operating system.
- Platform as a Service (PaaS): The user uses the cloud as an environment for executing applications. This is the opposite approach from SaaS, because users control their applications but have no control over the operating system, network or hardware on which their applications execute.
- Infrastructure as a Service (IaaS): This is an even higher level of abstraction. Rather than purchasing servers, software, memory, or networking equipment, the user accesses its necessary resources as a fully outfitted service from a third party, typically on a pay-per-use basis.

Virtual Systems (NCE $)/Cloud (NCE $) may occur at many levels (e.g., hardware, memory, storage, software, data, desktop, network, or entire data centers). Virtualization at the level of the operating system (OS) permits the hosting of multiple virtualized environments within a single OS instance. Applications can be virtualized, allowing them to be hosted independently of the underlying OS. Cross-platform virtualization allows software written for a specific central processing unit (CPU) and OS to nevertheless operate on different CPUs and OSs. At the top level of abstraction, a Virtual Machine (VM) is a software implementation of an operating system or computer. At the network level, virtualization allows access to applications, data, and computing resources through the Internet (also known as "cloud computing"). Cloud computing allows the user to move from a desktop model of computation to a network-based model.

For reasons of security and governance, clouds can be deployed as public, private, or hybrid. Public clouds are those data centers outside a user's firewall and are provided by third parties. Private clouds remain within a user's firewall; hybrid clouds offer a mixture of both.

From a security point of view, virtualization has issues with configuration management, patching, cross platform attacks, and auditing. Cloud computing has issues with shifting applications, data management, and processes to a third party set of configuration standards, control/ownership over sensitive data, reliability of company hosting the data, applicable laws (i.e., U.S. vs. EU privacy laws are very different), and lack of physical control. Security and confidentiality are crucial issues for successful transition to these technologies. In addition, there are legitimate concerns over performance variability, reliability, and resilience of cloud-based services. This is where the market is moving and we need to build security in upfront. Cloud computing consolidates resources and can become a cyberspace "center of gravity" for military organizations.

Intrusion Detection Systems (IDS)/Intrusion Protection Systems (IPS) (NCE $$) are the monitoring of the network to detect signatures of known malware or patterns of activity that are unauthorized. Today, significant attention is paid to protecting our IT systems to prevent intrusion. The philosophy underlying this is that if only authorized individuals have access to the IT systems, those systems are to a large degree protected. The philosophy driving interest in intrusion detection is that if no intrusion is detected, then it can be inferred that only authorized individuals are accessing the system and the system is *de facto* safe (clearly, per our earlier discussions, insider threat does not go away). However, ignoring the challenges represented by insider threat, Intrusion Detection is in itself a challenging problem. Today most security detection systems are signature-based, yet signature-based defenses are inherently perimeter-focused and state-of-the-art cyber threats tunnel through or go around these defenses. Also, Intrusion Detection Systems only show what they catch, not what they are not catching, so if there is no signature in place, the attack may go completely unnoticed. Looking forward we must detect/protect against zero-day exploits and move away from signature-based systems. IDS technology is not good enough to fight the APT, the military needs to move to advanced defensive techniques.

Skills

Massive Data or as it is more commonly being called today *Big Data* (VD $$) is the result of so much data being collected that there needs to be a way to stop data mining and start real-time correlation. Today logging is a challenge; the classic debate is how much needs to be done because it raises costs. Most large networks (over 10,000 users) do not have the resources to log more than a few weeks worth of data and even that is not truly analyzed. We need systems and processes that allow us to do long-term trend analysis (over months not just days or weeks). The military must analyze and react to data faster than their enemy. This will require more automation and intelligence systems.

Poor Interfaces (D $) are problematic as most systems are not designed to allow a user to rapidly manipulate information at the rate it is coming into the database. Those who have ever been in a Security Operations Center know it is not unusual to see Intrusion Detection System (IDS) events scrolling off the screen. The analyst is not able to control the process and must depend on correlation rules that the vendor developed so they cannot tell their managers what events they are getting are based on. We need security systems that are intuitive and allow the analysts to develop and manage the investigations in a way that they provide an advantage rather than just a person to react to what they are provided.

People

Threat/Risk Awareness (ED $$) is a concern because most users today implicitly trust their computer system when they log on, they assume emails are from who the email names in the "from" line and they do not think attachments like word documents could contain malware. This behavior issue must be addressed. We need to change the mindset of the user to "trust but verify" when they log on. Users should understand how to validate their security and know what kind of indicators to look for in a compromised system. We do not expect everyone to become a cybersecurity expert but we do want them to have basic survival skills to keep their information secure. One simple example is to use encrypted email when discussing sensitive material. There needs to be a national program; for awareness it could be based on the "Smokey the Bear says: stop forest fires" or "This is your brain on drugs" campaigns.

Insider Threat (NCE $$) is quite possibly the greatest challenge. There is no clear definition of who is an insider is. Most people automatically think an insider is an employee, a student, or other member of the staff of a host institution that physically operates a computer system. These people have a legitimate reason to access the IT systems and can be considered insiders. However, it can be many other types of people:

- A contractor, associate, business partner, computer maintenance technician, computer supplier, or someone who has a formal (or even informal) legitimate business relationship with the institution that hosts the computer system.
- An authorized person that is allowed to perform limited operations (e.g., a bank's customer who uses the bank's system to access his/her account or a student who is allowed to access grades).
- A spoofed authorized user.
- A person who has been coerced or even duped by an outsider to perform certain operations on the outsider's behalf.
- A former insider using previously conferred access credentials that were not revoked when the insider status terminated.
- A former insider who created "secret" credentials while working as an insider to give his/her access at a later date.

There are many reasons why a person behaves in a malicious manner. Some of these are for ideological reasons: revenge, ego that proves the insider can just do it, and plain greed. While people have not significantly changed in the last 20 years, the technical and economic landscape of the U.S. has changed significantly. Technology advances and e-commerce have made it easier for the insider to gain access to critical information [18]. This problem will continue to get more complex as the world becomes more interconnected. We need to increase our ability to use role-based management and real-time auditing.

WARNING

The precedent setting WikiLeaks case involving U.S. diplomatic cables [19] is the act of an insider that poses a new kind of threat. In the past we had people who were disgruntled, or had criminal intent, but now whistleblowers and hacktivists pose a new danger. This new potential breach of confidentiality could impact political systems, financial systems, and average companies with sensitive material. It will require a new set of processes, skills, and tools to address.

Skill Shortage (NCE $$$) is influenced by the general lack of skilled cybersecurity engineers today and the poor pipeline for new talent coming out of the schools. In the report "Human Capital Crisis in Cybersecurity," Jim Glosler a NSA visiting scientist and founding director of the CIA's Clandestine Information Technology Office was quoted saying "There are only about 1000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace: however the United States needs about 10,000-30,000 such individuals." There is a severe shortage of skilled cybersecurity professionals to address the needs of the force today, as many of the U.S.'s top cybersecurity minds are "unclearable" or have no interest in working for the government or the military. Also, educational programs focusing on cybersecurity at institutions of higher learning are still in their infancy. For the workforce challenge we should look at the Sputnik Moment the United States had when it realized they need a more Science, Technology, Engineering, and Mathematics (STEM) based workforce. There is some effort underway. In March of 2010 the U.S. administration did kick off the National Initiative for Cybersecurity Education (NICE) [20] and DHS/NSA have the Centers of Academic Excellence in Information Assurance Education [21] to help address this challenge.

Organization

Stovepipes (D $) are built around Computer Network Operations (CNO) functions of attack, defend, and exploit today. While it may be easy to separate different "disciplines" of cybersecurity for discussion points, they are all interrelated to one another in operational practice. These stovepipes are built around organizational structure, budgets or legal regulations. They are joking called "cylinders of excellence" by many in leadership positions who are trying to change the stovepipes but it very difficult to change as the organizational structure and budgets are built around them. When we look at Computer Network Operations, which consist of Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE), we see them treated as separate disciplines and there is little to no cross-talk or collaboration. Part of the challenge is much of the information for each aspect of CNO is classified at different levels. All three disciplines need to integrate the offense lessons learned (CNA) with the defense (CND) and enable them with intelligence (CNE). The DoD does this today in the kinetic world and needs to apply the same processes to the virtual battle space across the different organizations that control these capabilities. There has been progress in the integration of CNO and the doctrine continues to evolve.

Exercises (D $$) are simulations designed to practice responses to cyber scenarios. When we look at the number and types of exercises today there is simply a lack of both focused and integrated exercises to understand the responses to a cyber event. One of the reasons cyber is not included in most current government national security and military exercises is that the exercises are very expensive and the goals are usually not centered on cyber issues; as a result, many leaders do not want to allow cyber events to have a huge impact on the exercise. Generally, the rules that limit current cyber exercises do not accurately reflect the level of impact cyber is expected to play in a real world conflict so organizations are not training as they expect to fight. So while cyber is considered to be another domain of warfare (others being land, sea, air, space), there has been no unifying doctrine to understand the various aspects of "cyberspace" or Tactics, Techniques, and Procedures (TTPs) that would come out of exercises. Note that there are some efforts like Cyber ShockWave and Cyber Storm but cyber needs to become a ubiquitous aspect of exercises.

Core (Impacting all Areas)

Attribution (ED $$$) for cyber is the process of determining who conducted an activity. There are three types of attribution in cyberspace: geolocation (used to facilitate kinetic strike or military attack), tracking a cyber identity (facilitates the intelligence community tracking activity of a specific person or group), or tie a person to the keyboard (facilitates law enforcement in criminal investigation). It is worth noting there are many technical attribution capabilities that are not used due to policy or legal restrictions.

The ability to identify, beyond a reasonable doubt, the originator of a cyber attack is essential to enable an effective and legal response. This is the key to deterrence or retaliatory policies. Given the virtual nature of the cyber challenge, collection of forensic evidence takes on a new life. What is the cyber equivalent of a fingerprint or DNA? What does the "reasonable doubt" threshold mean in a virtual world? To complicate things further, if investigators are able to trace an attack, what can be done with the results? For the military what level of intelligence is sufficient to authorize and attack? Fundamentally, today there exists no way to reliably identify the original attacker.

In his 2010 testimony before Congress, General Alexander stated that: "Conflict in cyberspace, moreover, is highly asymmetric. Minor actors can afford and deploy tools to magnify their effects; witness the recent press reports about arrests in Europe of several individuals charged with creating the so-called 'Mariposa botnet'—a collection of 13 million computers slaved together for criminal purposes. The tools these actors can employ are almost anonymous—a defender can sometimes learn where an attack came from, but can be time-consuming. That means 'attribution' in cyberspace is costly and comparatively rare. The 'price' an adversary pays for a capability—a tool or weapon—can be slight; the cost and impact borne by the victim of the attack can be very high" [22]. This comment is still relevant today.

Deterrence (ED $) is associated with what will happen if we launch a cyber attack or practice poor cyber behavior. Deterrence only occurs when there is something, such as a legal rule, cultural taboo, or consequence that makes us not "attack" a system, knowing full well what happens when we get "caught." The most critical aspect of deterrence is to make the cost/benefit ratio change from today's high benefits and low cost or risk to us to where the costs outweigh the benefits. This can be accomplished by making the cost of the attack too high by either increasing the barriers so that an effective attack requires significantly more resources to perpetrate, or by increasing chance of detection. In an economic example, deterrence could be preventing spam email by charging one-tenth of a cent for each email; this would not impact normal users but would make spam email too costly. A military example would be a counterattack (virtual or kinetic). A technical example would be to find and block the threat so quickly it is not practical try to maintain a persistent presence on the target network.

Situational Awareness and Visualization (ED $$) is the correlation and fusion of data from multiple sources that enables decision making. This is, at best, poorly understood today. Situational awareness allows leaders to make informed decisions. There are many Common Operational Picture (COP) tools and dashboards today, but they fail to facilitate true risk posture understanding and/or provide information in a format that enables decisions. If the data does not facilitate a decision it will soon be ignored. The types of data and their presentation should be driven by the types of decisions that must be made. It will vary at different levels of an organization and for different functions within any organizational level but today they are driven by the type of data available. First the roles need to be set, and then we must understand what decisions need to be supported. Finally the standards for implementing how we present information to the different audiences need to be established. This is a fundamental capability for command and control within the military.

Lack of Common Taxonomy (VD $) issues revolve around the need for a standard "language" for cyber topics. When we read or discuss computer security, network security, InfoSec, Information Assurance, cybersecurity or cyber war, we must be careful to understand the terms that are being used and that everyone is using the same definition. There is no governing industry standard, government regulation or international agreement on what is meant by simple terminology like "intrusion." This lack of a governing body establishing a common baseline of definitions makes interaction between organizations problematic. This can quickly lead to confusion when trying to have a diverse group of professionals analyze an incident. Within DoD there was so much confusion on what malware was called they hired MITRE to establish a Common Vulnerabilities and Exposures (CVE) [23] database. There needs to be an international body that determines the definitions for IT terms that will be used by the technical community, governments, and the legal authorities. The military is working to standardize this between U.S. service branches and internationally to allow clear communications.

Information Sharing (D $$) is a challenge in the sense that people like to share most information with the exception of what they believe to be private. However, this is not the case for governments and corporations. Corporations often do not share information simply due to competition, and governments do not share information for matters of national security. In the cyber world, the question arises whether corporations and governments should share information on cyber attacks. There are over 30 programs attempting to do this today as well as governmental and legislative efforts but they are challenged by concerns over liability, brand protection and value provided based on the cost of participating.

However, there are cases where we may want to keep cybersecurity issues limited to a few key personnel. Some examples of these cases are: do not want to expose a vulnerability, desire to protect reputation, need to limit liability or cost of participation in external investigation. Efforts in one area often do not share information with efforts in another despite being interrelated. Knowledge transfer in a large organization is more difficult due to the size and communications flow. There are also a number of public/private efforts that the government is trying to get industry to share information but these efforts are not coordinated and many of them are only achieving limited success.

Note that the WikiLeaks' release of hundreds of state department cables was not an Info Sharing issue, but rather an Insider Threat issue of someone motivated by what we would call hacktivism. Organizations often do not systematically review their processes to prevent internal cyber attacks. They need to review industry best practices, internal and external, in order to improve organizational performance. They need to conduct after action reports or lessons learned to conduct sharing with the appropriate level of risk.

Metrics (D $) revolve around the need to quantify the impact of malicious and suspicious cyber activity. Just as there is no common understanding of definitions for cyber topics, there also exists no set of predefined, industry standard metrics for cyber activities. Metrics for cyber are difficult to implement because of varying definitions of what is needed and important. For example, how we measure Return on Investment (ROI) is varied based on what organizations see as important. There are three basic types of metrics:

- Technical: Most organizations track how many intrusion attempts were stopped, how many viruses were detected, number of days/hours systems were up, communications exchanged (email, IM), number of incidents closed out.
- Security: If an organization introduced new processes to detect intrusions that increased detection by 20% or lowered cost by $50,000, or introduced a new tool in the Security Operations Center that cut time to accredit systems by 17 weeks. These goals must be set before the change and methods to track performance are established.
- Risk Posture: Examples include: when an organization is connected to new partner networks and it impacted our risk by 40% or our external router was compromised and it lowered our security posture to yellow because it forced us to change the access control list to block IP ranges that were attacking us without normal configuration control processes.

There are many groups working on this issue to include the Administration's CIO's IT Dashboard and the IT Workforce Committee's Importance of Effective Performance Metrics studies, but these are not getting the level of wide acceptance needed [24]. The solution may be regulatory, legislative, or industry best practices, but there needs to be a standard so we can measure the impact and benefits of our actions. A great resource that has been developed by MITRE is the "making security measurable" project. [25] They have a Common Weakness Risk Analysis Framework with supporting threat-based analytical programs.

System Integration (D $$) is the desire to overcome the common practice today of an organization purchasing multiple point security systems that do not work together and instead, get one system that coordinates and correlates protection activities. Most security systems used today have a specific function. For example, an organization may have a firewall, an intrusion detection system, anti-virus and anti-spyware tools, forensics tools to help with attribution, network management and monitoring systems including packet sniffers, encryption/decryption capabilities, virtual private networks, patch management systems, web activity filtering, password, and log activity correlation. Each of these systems produces logs which need to be correlated together to provide a view of the overall system health and risk posture. This type of correlation is only possible through the appropriate integration of our subsystems and is essential to address a variety of cyber threats including the ability to identify and track potential insider threats. However, too often today's subsystem act as a series of point tools that do not interact to achieve the synergistic effects integration can provide.

It should be noted that, while systems integration can provide numerous benefits, including enabling a more complete and integrated operational picture of the cyber threat, it also increases the risk that, like dominos, an effective cyber attack that brings down one subsystem causes the entire system to fail. This highlights the importance and need for resilience and represents an important challenge in architecting the cyber enterprise. Just as in insurgency warfare, there is a trade-off between pushing down control to the lowest levels to allow small units to act independently versus having more centralized control to enable larger coordinated efforts. Likewise, the architecting of a robust cyber enterprise faces similar challenges. We cannot continue to have multiple point solutions, we need a unified framework.

INTERRELATIONSHIP OF CYBERSECURITY CHALLENGES

Many of these issues are interdependent. We will follow some examples of how they are tied together. The following examples will highlight some of the interrelationships between the issues.

Deterrence is something the United States uses as a foundational part of their foreign relations policy. There have been many discussions about how this principle can be applied to cyberspace. Before we can begin to utilize deterrence we require attribution pointing to a specific individual, group or nation that is responsible. If we are able to solve this (through use of all our intelligence capabilities) we would still need clear policies on our reaction, military doctrine and ROE showing our responses. This would not be a simple if A then B equation like the Nuclear Mutually Assured Destruction (MAD) policy, as there is a wide range of factors that could come into play. It would be more like a complex matrix of options which is hard to use as deterrence because the response is often not clear.

Military ROE is complex for the same reasons deterrence is difficult. There would need to be a clear set of actions with easily understandable reactions preauthorized. National policy, supporting laws and doctrine would all need to be established. Finally standards of attribution would need to be determined so commanders could know when they had enough intelligence (military normally acts on intelligence and not the legal requirements required for evidence to be presented in a court of law) to act.

Mobile devices would require a set of common interfaces to allow system integration. There are so many proprietary systems using unique protocols and configuration that it is not practical or cost-efficient to have one network operations center or security operations center try and manage them all. Some advancement in systems integration is needed to allow the management of all the devices being introduced to networks every year.

Audits are becoming critical to risk management, but it depends on developing industry standards. Before these standards can be created we need to baseline the identity management systems, agree on what metrics will be analyzed and document the definitions of everything involved.

Stovepipes are tied to Classification of Data. Stovepipes are organization-based issues but the culture of classification of data is normally set inside the same stovepipe. Once a culture of sharing is established and the walls are broken down the culture of what can reasonably be declassified will allow the release of a lot of information. It is important to note that insider threat is also a key concern when establishing a functional system for sharing information. Auditing and good identity management (both authentication and authorization) are the foundation for building a system that allows safe sharing of information.

Situational Awareness is the "holy grail" for many large networks. It can mean understanding what the attacker's intent is, what they have done after they got in, how an event has changed the risk posture of the network, what the impact to mission capabilities or identifying who it was that penetrated the network. Each of these questions requires a slightly different set of data to answer the question. For some it is just correlation of the integrated systems, for others it is metrics, some require internal auditing, a number of them want attribution. The data must facilitate a decision and be presented visually in an intuitive manner.

Insider Threat needs policy support, auditing, and identity management. First, privacy issues need to be addressed. Then we have to find a cost-effective way to track activity of all users and be able to recognize malicious behavior. Finally, we have to be able to positively identify who took which actions. These must all be solved in a standardized and cost-effective way which requires solving the auditing set of issues and situational awareness issues.

Then there are the issues that involve multiple challenges. To some degree they are all impacted by lack of taxonomy, metrics, and the standard rules (doctrine, policy, regulations, procedures, standardization, laws, etc.). It is very difficult to have a discussion about the solution if there is not a common baseline on the meanings of terms and methods or measurement much less without common set of guidelines everyone will follow. Finally, supply chain underlies all of the technical issues. If we cannot have confidence in our hardware or software then nothing that happens can be believed.

WAY AHEAD

What should we focus on with limited resources? Some of these issues require national policy/legal guidance (if not international agreements) others are tactical in nature and can be fixed at lower levels while still others require technical innovations for new solutions. Let us look at what level the issues resides at.

At the international level we need agreements and processes to address attribution, supply chain and legal issues. At the national level the government needs to set a consistent and interconnected policy/legal strategy, set up governance for standardization of taxonomy and metrics, publish our policy on deterrence, doctrine (with ROE), and expand our development of the skilled work force we need through both training and exercises. To do this we have recommendations on organizations at the U.S. national level that should be the lead for specific missions:

- U.S. Congress should set the course for national policy and legal statutes and assign/resource many of the roles discussed here.

- NIST should focus on taxonomy, metrics, and auditing. They could establish standards for virtualization, cloud computing, data protection, insider threat protection, system integration, and mobile device management.
- DoD should develop doctrine with ROE. They would need to build ways to develop chain of trust and mission assurance for key command and control as well as weapon systems. They require a core of service members with cyber warrior skills through training and exercises. They are in a good position to address the classification processes and stovepipe issues.
- DHS should focus on situational awareness, identity management, IDS/IPS, IPv6 implementation, and dealing with massive data. They would also be the lead for national program to increase risk awareness and developing the skilled workforce we need.
- DoS should be the lead for developing deterrence strategy and building international agreements.
- DoJ should focus on policy and legal enforcement of the laws we have.
- Organizations like Federally Funded Research and Development Centers and Defense Advanced Research Projects Agency (DARPA) should focus on resilience, chain of trust, attribution, and supply chain.

This assignment of challenges is extremely basic and does not represent a clear mapping of missions of the different agencies/organizations. These organizations would all need to work closely together so they would not get stovepiped on their own solutions set. We have left out players like White House CIO, CTO, and Cyber Security Coordinator as they do not control significant resources. We did not include DoE who is working cybersecurity for smart grid technology. This list was just a sample but reflects some of the intricacy involved with these issues, a more detailed study would need to be done with specifics based on a scenario to get a more complete list. It is meant to be more of a starting point to allow everyone to weigh in on which issues belong to each organization. It is clear the current distributed and poorly coordinated efforts are not proving to be effective enough to position the U.S. to maintain their current level of influence in cyberspace. We need a national roadmap that assigns responsibility and resources to address these concerns.

Another way to categorize these challenges is to look at a rough timeline to solve them (understanding that resources determine if and when they will be solved). So, with no crystal ball, here is a prediction on some of the issues. In the next 5 years doctrine should be well established based on the current activity in DoD, though ROE may not be defined very well. There will also probably be new laws based on the number of bills in Congress. Many technical issues like virtualization, cloud computing, identity management, data protection, massive data analysis, and situational awareness are all being heavily invested in and will see major improvements. Expect to see cyber being included in more exercises and cyber centric exercises to become more common. IPv6 will force its way onto center stage and become a standard protocol—time will tell how much it solves. There are organizations, both inside the government and commercial industry that are working on metrics and auditing so we expect major improvements but it is doubtful there will be any global standards established.

Then there are issues that will be worked on over the next 10 years but it is doubtful there will be a clear solution without significant effort: taxonomy, attribution, deterrence, the shortage of a skilled cyber work force, risk awareness, and systems integration. These issues are so complex and today there is no clear champion to drive them to closure that it is hard to see them being worked out. Looking long range the level of research will determine which issues will be cracked but we would hope to see resilience, chain of trust, poor interfaces, and supply chain addressed.

For those cross walking all the issues we listed there are some we did not talk about because we are unclear where they could fit so did not try and make a prediction.

SUMMARY

The United States faces multiple security challenges today competing for limited resources. However, one of them is woven throughout the rest and is vulnerable to attack from everyone from a lone individual to a nation state: cyberspace. There are a number of organizations trying to solve or profit from these issues but there is no critical mass to enable real progress on any of the key issues we have covered in this chapter. The national and international debate on cyber needs to determine what we must address as many of these issues have a long lead time to solve. We need a leap ahead effort to introduce game changing technology or change the rules we play by with new policy or even morph the game board by a paradigm shift in the underlying infrastructure of the Internet.

References

[1] Obama B. Remarks by the President on securing our nations cyber infrastructure. The White House web page, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure; 2009.

[2] IP3 National Cyber security R&D Challenges. http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf.

[3] National cyber leap year, http://www.nitrd.gov/leapyear/RFI_LeapYear.pdf.

[4] InfoSec's hard problem list, http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf.

[5] Four grand challenges in trustworthy computing, http://cra.org/uploads/documents/resources/rissues/trustworthy.computing_.pdf.

[6] DoE A scientific R&D approach to cybersecurity, http://science.energy.gov//media/ascr/pdf/program-documents/docs/Cyber_security_science_dec_2008.pdf.

[7] Securing cyberspace for 44th president report, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[8] President's Critical Infrastructure Protection Board. http://georgewbush-whitehouse.archives.gov/pcipb/ [accessed 17.12.10].

[9] Comprehensive National Cybersecurity Initiative (CNCI) focus areas, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[10] Obama's Cyberspace Policy Review. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [accessed 17.12.10].

[11] James E. Cartwright vice chairman joint chief of staff. Cyber reference library. National Security Cyberspace Institute, Inc. (NSCI), http://nsci-va.com/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[12] CSIS: 20 critical security controls version 4.0, http://www.sans.org/critical-security-controls/.

[13] NIST. Special publications (800 series), http://csrc.nist.gov/publications/PubsSPs.html.

[14] DHS stop – think – connect program, http://www.dhs.gov/stopthinkconnect-key-cyber-issues.

[15] Wulf WA, Jones AK. s.l. Reflections on cybersecurity. Sci. Mag. 2009;326(5955):943–944.

[16] NIST publication site, http://csrc.nist.gov/publications/PubsSPs.html.

[17] DHS. http://www.nist.gov/nstic/.

[18] Stern-Dunyak A. Insider threats: countering cyber crime from within. MITRE, http://www.mitre.org/news/digest/homeland_security/10_09/cyber_crime.html.

[19] Shane S, Andrew WL. Leaked cables offer raw look at U.S. diplomacy. New York Times. http://www.nytimes.com/2010/11/29/world/29cables.html?_r=4&bl=&adxnnl=1&adxnnlx=1292778173-fMW1SzDCUGvclejwT3KnJA&pagewanted=all; 2010.

[20] NIST. National Initiative for Cybersecurity Education (NICE), http://csrc.nist.gov/nice/.

[21] NSA. National Centers of Academic Excellence, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

[22] Alexander KB. Statement to house committee on armed services. DoD, http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf.

[23] MITRE. Common vulnerabilities and exposures (CVE), http://cve.mitre.org/ [accessed 01.01.13].

[24] CIO, Steven VanRoekel U.S. CIO homepage, http://www.cio.gov/; 2010 [accessed 02.01.13].

[25] MITRE ‘making security measurable’ project, http://makingsecuritymeasurable.mitre.org/index.html.