THE RAPID CYBER THREAT:
EVOLVING THE DEFENSE IN DEPTH STRATEGY FOR NATIONAL SECURITY SYSTEMS

A CASE STUDY SUBMITTED TO
THE ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION
AND
CYBER CONFLICT STUDIES ASSOCIATION

BY

PHILIP W. ROBBINS

JUNE 2012

Disclaimer: The views expressed herein are the personal views of the author and are not intended to reflect the views of the Department of Defense or U.S. Federal Government.

Introduction

Today, more than ever before, knowledge is being characterized by power. Further, it's the secrecy of knowledge which allows for both power and control. While knowledge isn't synonymous with information, we certainly live in an age that is driven by it: an information-centric age of modern communications and global interconnectedness, where information is stored, transmitted, and accessed near the speed of light, by anyone, anywhere, at anytime. As such, this transformation of our communications landscape has created an escalating challenge for the security of National Security Systems (NSS), that safeguard our most sensitive and classified information. Ever since World War II, and the development of the atomic bomb, the United States Government (USG) has had a need to keep secrets (power and control), over its adversaries, in the interest of national security. Over time the proliferation of secrets has increased, almost proportionally, to the very technologies developed for the purposes of gathering and processing such information. That information has always been, and up until recently, the target of a rapidly growing threat within our newest military realm, dubbed as 'cyberspace' – a term, adopted by the USG, to describe the global network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems.

Earlier this year, FBI Director Robert Muller testified before the Senate Select Committee on Intelligence soliciting help to combat what he believes is becoming the Nation's number one threat, saying that 'the cyber threat will surpass the threat from counter terrorism.' How is this rapid cyber threat actually being measured? One way is through incidents that are reported to the United States Computer Emergency Readiness Team (US-CERT), where both the number of vulnerabilities and incidents are tracked and recorded annually. However, because cyber threats have become so commonplace, its near exponential growth has caused US-CERT to abandon tracking incidents since 2006. Based on existing data, plotted and shown below in Figure 1, representing an increasing probability of occurrence, reveals that by the end of the year 2012, there would have been more than an estimated half a million cases of cyber related incidents.

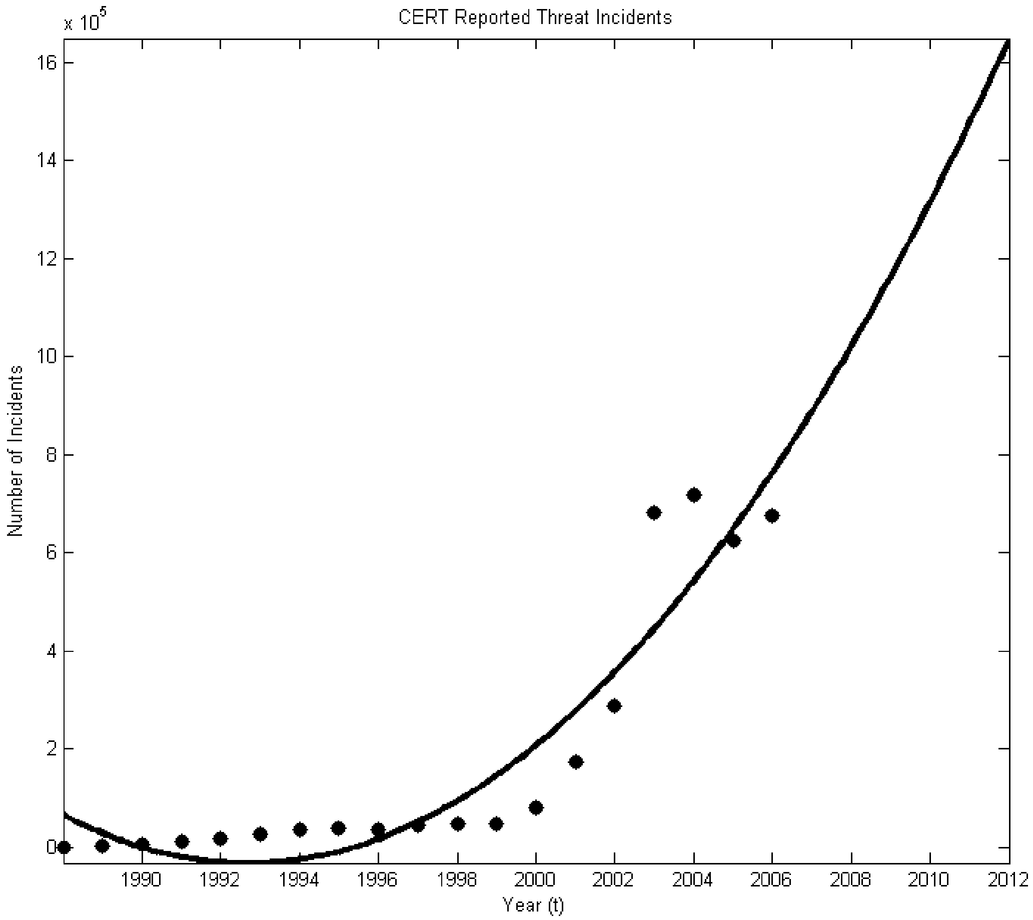

Figure 1. US-CERT Cyber Threat Incident Plot

Dealing with cyber threats is a multifaceted situation, where the spectrum of malicious individuals or groups conducting attacks includes actors, labeled as advanced persistent threats (APTs), who use creativity, intellect, and motivation to bypass and adapt to security measures.

With Information Assurance it does very little to script a response to an attacker the same way a system administrator would respond to an IT issue. Certainly, no one can protect against everyone and everything, however, a comprehensive and optimized security strategy, flexible enough to adapt and evolve as these new APTs emerge, must be used.

Today, Defense in Depth (DiD) is a practical strategy that is used for achieving Information Assurance. DiD is not a product or even a suite of network security appliances, but a ‘best-practices’ strategy - a proactive approach utilizing people, technology, and operations - looking at security from the inside outward, while balancing between protection capability, cost, performance, and operational considerations. The National Security Agency (NSA) defines DiD as a layering tactic which implements multiple layers of defense to delay security breaches - buying time to detect and respond to an attack, rather than preventing individual attacks to critical systems. DiD is able to coordinate the use of multiple security countermeasures, within an enterprise environment, providing redundancy when a security control fails, or protection when a vulnerability is exploited. A common analogy is often made between the DiD strategy and the layers of an onion.

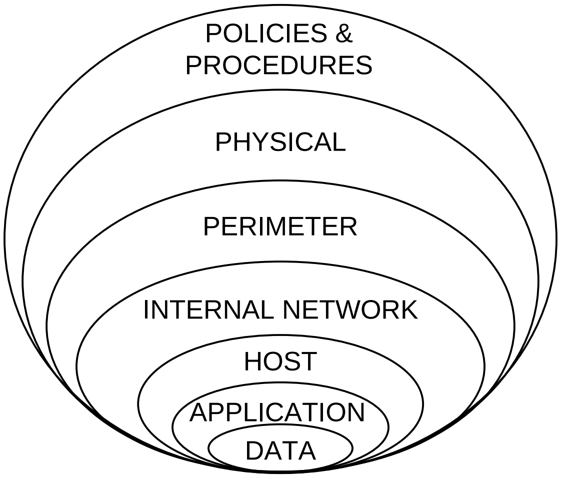

Figure 2. Layers of Defense in Depth

Review

On July 15, 2010, the country of Iran became the first victim of cyber war in history, as the world was introduced to the most sophisticated, advanced computer worm ever detected and the first cyber weapon of its kind: W32/Stuxnet.A. The Stuxnet cyber weapon is made entirely out of code, and was considered an attack to have crippled Iran's nuclear plans by altering and exceeding the maximum rotation speed of centrifuges that were spinning nuclear material at a heavily fortified, top-secret, underground, uranium enrichment facility at Natanz, further leading to the closure of the Bushehr Nuclear Power Plant.

Stuxnet is considered a worm opposed to a virus because of its ability to self-propagate through networks and execute on systems on its own. It targets pieces of code that monitors critical factory operations – highly sensitive components with millisecond response times – preventing operators from ever noticing any changes, thus, allowing the nuclear refinery's centrifuges to malfunction undetected. Stuxnet didn't attack every computer it infected. In fact, it was written to hit only one specific target in the world. After infecting a computer, Stuxnet constantly checked to see whether the parameters for launching an attack were met – seeking to destroy a specific type and configuration of equipment systems, including Iranian components not used anywhere else, at a specific time, and at a specific facility – while otherwise remaining relatively dormant for the right conditions to present itself (Mitchell, 2011).

Stuxnet was designed with several purposes in mind. It sought to (i) seize control of computers covertly by gaining privileged access, (ii) spy on infected systems by capturing and exfiltrating data, (iii) compromise supervisory control and data acquisition (SCADA) systems by reprogramming circuit programmable logic controllers (PLCs), and (iv) sabotage and circumvent safety mechanisms used to control and monitor the industrial systems. Stuxnet is believed to have been able to bypass many robust physical security measures at the Iranian nuclear facility, through the use of a USB thumb drive, allowing itself onto the isolated (closed) network while covering its tracks. The code reveals that after infecting three new devices, it removed itself from the original device, self-replicating without the use of the system's autorun feature.

Written in multiple programming languages, the Stuxnet code contains an impressive array of capabilities, thanks in large part to a payload considered nothing short of rocket science; combining logic bombs, root kits, spyware, and exploitation of security gaps system creators were unaware of (zero days), including code allowing mutation and creation of multiple variants of itself, all while digitally signed with certificates that were stolen from some of the most reputable computer technology companies in the world. Many security researchers believe that, up until now, other notable attacks seen before Stuxnet have all been child's play in comparison. Until now, despite an increasing amount of suspicion, there was no definitive proof identifying the originators of Stuxnet. Detailed analysis of the code, by experts reveals that, its carefully constructed design, development, and successful facilitation would have required the full technical knowledge, details, and resources of a politically motivated nation state or group of nation states. Intelligence leaks ultimately lead U.S. officials to confirm that Stuxnet was created by the U.S. and Israel as part of operation Olympic Games under the administration of President George W. Bush.

The release of Stuxnet, by most accounts, was considered to be successful in setting Iran's nuclear program back several years. However, at what cost? By the very nature of its design, Stuxnet was never meant to be seen, let alone, come to the public's attention. It was meant to be kept secret, running undercover, while hopefully remaining undetected. It was to go unnoticed up to its kill date of June 14, 2012, when it was scheduled to automatically delete itself, removing any trace of its existence, thus eliminating the possibility of its code ever being discovered. Nine months after being detected, the first virus that could potentially cause power grids to crash or even oil pipelines to explode is now readily available online for anyone to download, study, and tinker with. The remaining question now is who will redesign it? You can read about people all over the internet pulling the ten-thousand lines of Stuxnet code apart. It has now become an open source weapon with no way of knowing who will use it or what they will use it for (Mitchell, 2011).

Before Stuxnet, cyber crime was generally limited to spam email, identity theft, and distributed denial of service (DDoS) against websites. The development and deployment of Stuxnet has ushered in an entirely new wave of cyber conflict – a wave of conflict in which a cyber weapon, consisting of binary digits (1’s and 0’s), can now used to cause destruction rather than simple disruption – and in the case of Stuxnet, physical destruction to infrastructure. Today many cyber security experts, and those in the highest positions of government and military, are branding this wave of conflict as an era of cyber warfare; one in which capabilities are needed to both defend against attacks, and launch our own. However, there are a wide range of unintended problems and potential risks associated with this new form of warfare.

If used properly, a physical weapon will destroy any traces of itself along with its intended target; however, a complex cyber weapon doesn’t share the same favorable behavior. Today’s rapid cyber threat includes APTs who would back track and reverse engineer code, such as Stuxnet, to repurpose a cyber weapon in order to launch a cyber attack against high value targets within concentrated and target rich environments including Japan, Europe, and the United States. A worst case scenario would involve an attack on a national security system that would take down critical infrastructure. Such an attack would be very difficult to restore in a short period of time, paralyzing our country, while causing enormous economic damage, and even loss of life. The Department of Homeland Security (DHS) specifically categorizes our critical infrastructures into eighteen sectors, of which contain notable services such as (i) water treatment facilities (ii) telecommunication lines, (iii) banking & finance, (iv) air traffic control, (v) oil & gas pipelines, (vi) electrical grids, (vii) power plants, (viii) chemical plants, (ix) nuclear facilities, and (x) military command & control systems (DHS, 2003).

The release of Stuxnet sent a message to the rest of the world that not only does this type technology now exist, but its creators are willing to deploy it, risking the consequences of a possible accident on a nuclear magnitude, or even retaliation in the form of a kinetic attack. As the most vulnerable and targeted nation on Earth to cyber attacks, the time has come to accelerate the development and refining of cyber strategies, programs, and capabilities, in order to both protect national security information and national critical infrastructures; combating the proliferation and future use of these weapons of mass disruption (WMD) by APTs.

Methodology

Security Risk Analysis quantitatively expresses an attack or compromise against a Critical Information System as a conditional event in which a threat class exploits a single or subset of open vulnerabilities. It is important to note these vulnerabilities are independent of any threat variable and exist within all Information Systems in operation. The risk of compromise arises from the potential loss of any, or a combination of the following, Information Security Services (ISS): Confidentiality, Integrity, and Availability (C-I-A). As an example, cyber crimes specific to denial of service attacks, including cyber weapons that cause physical destruction to critical infrastructure, are directly tied to the loss of the ISS associated with Availability.

A Risk Management Framework (RMF) is used to assess risk based on the likelihood of negative consequences or loss from the exploitation of a vulnerability. Performing risk assessments and adjudications for national security systems allows for the evaluation of actual impacts, appropriate corresponding control measures, and mitigation techniques. An organization does not implement fingerprint readers, firewalls, backup systems, or any other safeguard just because they should have it. Risk is ultimately a business concept, and as such, the ramifications for not implementing such safeguards must first be understood, and considered given resource constraints.

It’s pointless to measure how many attackers are actively targeting you, as it is considered impossible to control the rapid and increasing cyber threat. APTs can leverage vulnerabilities in people, computing systems, and communication networks; representing a massive potential target landscape to protect from edge to edge. No single solution provides this type of comprehensive security (Rosenquist, 2008). However, it is possible to manage existing vulnerabilities through containment, information assurance principles, and Defense in Depth strategies. The most viable method of approach is to assume that you have been compromised and focus on how to respond.

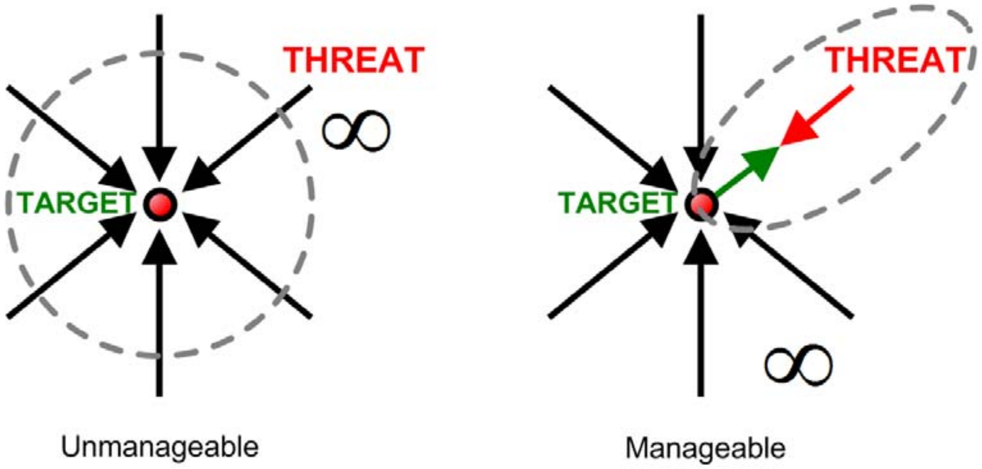

Figure 3. Threat Approach Profiles

DiD requires a balanced focus on three primary elements: People, Technology, and Operations. The first line of defense typically begins with the *people* who establish and enforce security measures. A top down approach starting with senior management, or Chief Information Officer (CIO), who understands the perceived threat. This is followed through with effective IA policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel, and personal accountability (NSA, 2001).

The DiD *technology* element includes network security architecture, products, and solutions such as adaptive security appliances (ASA), firewalls, data management zones (DMZ), virtual private networks (VPN), intrusion detection systems (IDS), access controls, and audit tools, that are used to support the layered defense strategy and maintain information assurance services. These technologies can be deployed in multiple places providing resistance from attacks targeting multiple points at the outer network and inner enclave boundaries.

The *operational* element of DiD focuses on all activities required to sustain an organization's security posture on a day to day basis, including (i) management of IT security posture through patching and virus updates, (ii) certifying and accrediting (C&A) IT baseline changes with process data used to support risk management decisions, (iii) keeping system security policies up to date, (iv) monitoring of logs, (v) incident response, (vi) recovery and reconstitution, and lastly (vi) periodic security readiness assessments (RED Teaming) of systems and networks to exploitation (NSA, 2001).

Information Assurance (IA) is achieved when information and information systems are protected against attacks through the application of Information Assurance Services (IAS). IAS are applied using an interlocking Protect, Detect, and React (PDR) DiD paradigm which goes beyond general protection mechanisms, and toward adopting an expectation that attacks will occur, and to include detection tools and procedures allowing reaction and recovery from them.

An effective *protective* countermeasure from the PDR DiD paradigm is the deployment of multiple defense mechanisms between the adversary and their target. Each of these mechanisms must present unique obstacles to the adversary, providing protection while increasing the chance for detection. *Detection* capabilities identify violations of policy, incidents, incursions, intruders, defense breaches, and the circumvention of security. This itself is becoming more challenging, as the trend is moving toward stealth attacks - system compromise without drawing attention - increasing the length of time attackers have on the system. When it comes to detection, speed and accuracy are important, and thus, focus must be placed on the right areas and events. Detection directly feeds into the reaction process and serves as feedback for protection; continually strengthening the overall security posture. Reaction requires a swift and effective response harnessing the resources of an entire organization to quickly contain, reverse, and recover from attacks. Capabilities should already be in place and have been tested in advance in order to effectively resolve and restore normal operations.

The security robustness (strength and assurance) of each information assurance component should be evaluated against the value of what it is protecting, as well as, evaluating the threat at the point of application (NSA, 2001). It is prohibitively expensive, and unmanageable to protect against every cyber incident. DiD is a sustainable strategy that ultimately reduces the frequency of incidents and costs over time.

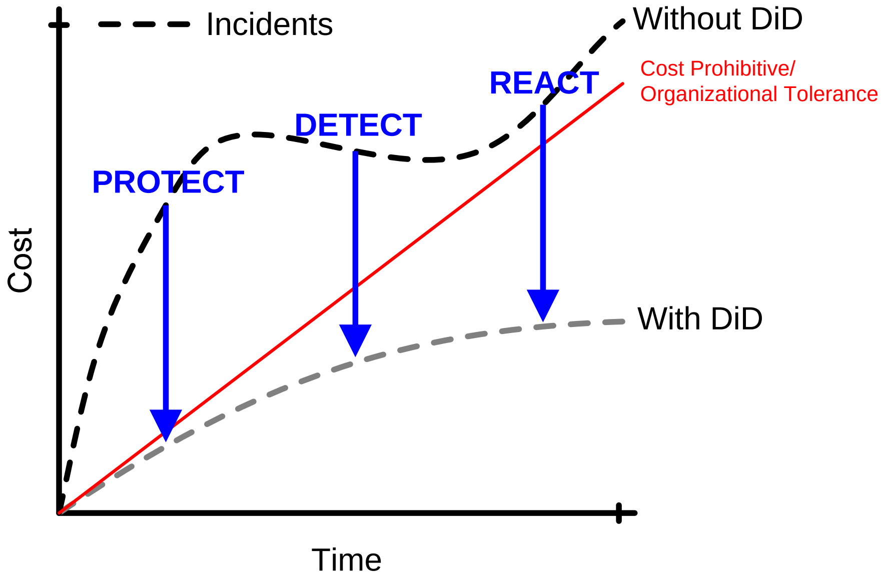

Figure 4. Cost per Incident over Time Relationship Before & After DiD PDR Paradigm

Information Assurance (IA) differs from information security, operationally, in that, additional emphasis is placed on information sharing, and the mechanisms for establishing and controlling trust amongst users, through authorization and authentication (Cieslak, 2009). The United States Pacific Command (USPACOM) Information Services Reference Model describes the following Information Assurance Services (IAS) as ‘the ability to protect and assure information and info structure' within the following seven categories based upon the revised Defense-in-Depth vision (Cieslak, 2011): (i) Physical Security, (ii) Cyber Security, (iii) Continuity, (iv) Security Design, Configuration, Operations and Administration, (v) Security Education, Training and Awareness, (vi) Identity Authentication and Authorization, and (vii) Information Content Security. The diagram below illustrates the support structure for Information Assurance and its relationship between the Information Security Services C-I-A Triad, Information Assurance Services, DiD PDR paradigm, and DiD primary elements.

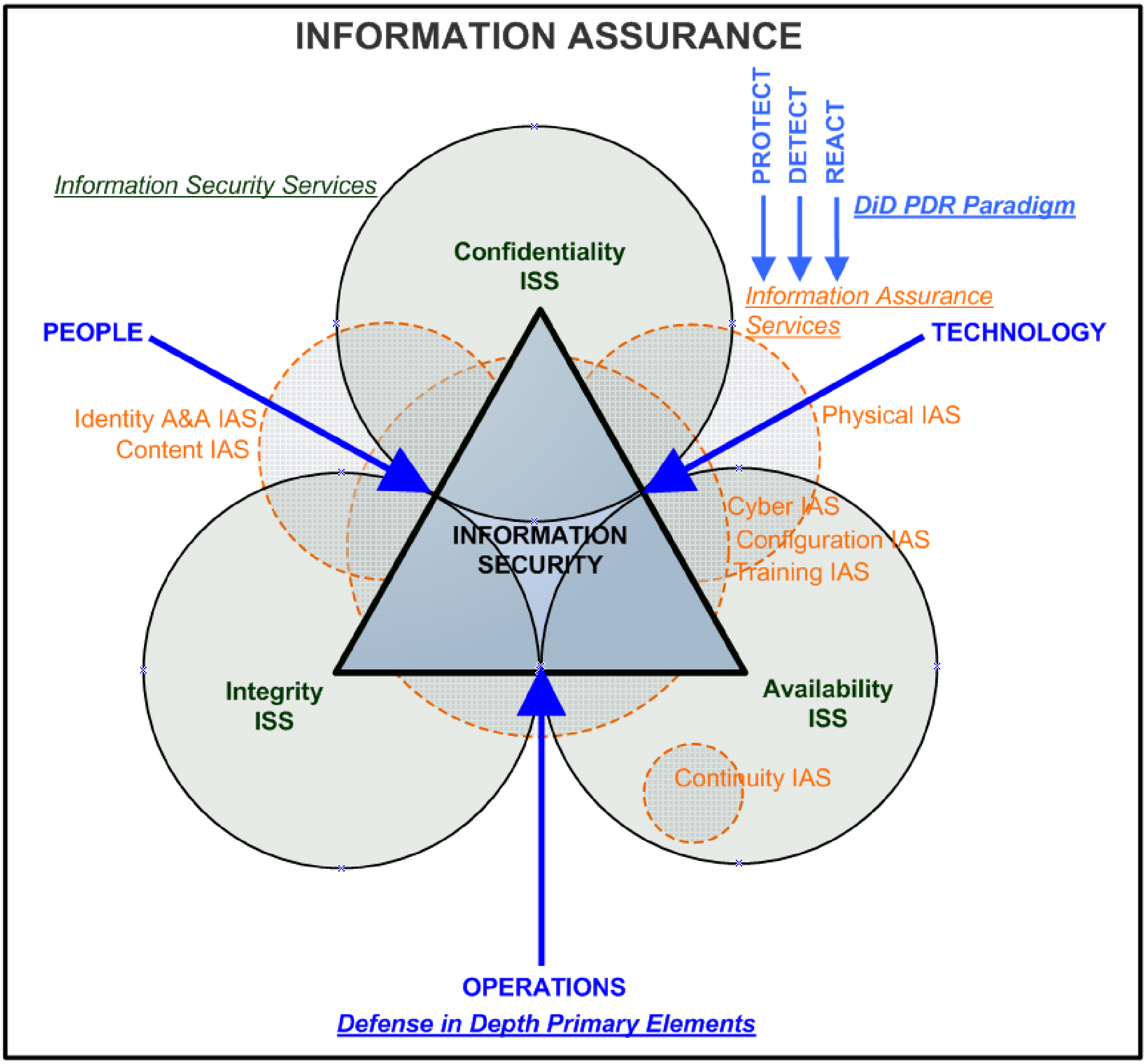

Figure 5. Overall relationship between Information Security, ISS, IAS, and Defense in Depth

Analysis

Those who protect national security systems and critical infrastructure have a responsibility to the public to protect those assets on their behalf. With the gloves now off we are bearing witness to an explosive growth within the cyber security and defense industries. Anticipated to reach $13.3 Billion/year by 2014, cyber security is one of the few areas receiving more money during a time when the U.S. defense budget is seeing targeted cuts. The President issued a sixty-day cyber review report, in which he made a commitment that "from now on, our digital infrastructure, the networks and computers that we depend on everyday, will be treated as they should be, as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks, and recover quickly from any disruptions or damage (60-Day Review, 2009)."

Cyber war has become a controversial subject, with some experts arguing that the whole idea is being overhyped, with fear and uncertainty used to cash-in on a booming and lucrative industry. Although the President Obama has allocated federal government spending for securing critical infrastructure, there is neither exaggeration in, nor underestimation of, the truthful state of vulnerabilities in our networks and at our endpoints. In a cyber war, your assets and the vulnerabilities inherit within them, become your greatest weaknesses. Are we exposed? Absolutely. It's clear that if defense in depth strategies weren't being implemented today, we certainly would be exposed to a host of cyber-related crimes, eventually leading to some form of cyber war.

The terms *Cyber Crime*, *Cyber Conflict*, and *Cyber Warfare* have often been used interchangeably and very loosely. Care must be taken when adopting words like ‘war’ when framing the cyber threat. To be clear, we are not in a cyber-war, however, there is a cyber-conflict. The difference between the two depends both on (i) which of the following types of cyber crime (crime using a computer and network) is involved: espionage, sabotage, and/or attacks, and (ii) the boundaries impaired by the crime: national versus regional, local, or municipal in scope. There is some contention on whether DDoS - a cyber crime which causes disruption – can enact an act of war or not. Certainly if a threat was acting with malice, then yes, this becomes a real threat that isn’t limited in scope just to websites. Disruption leading to the failure of emergency communication systems and services (i.e. 911) can directly result in the loss of human life.

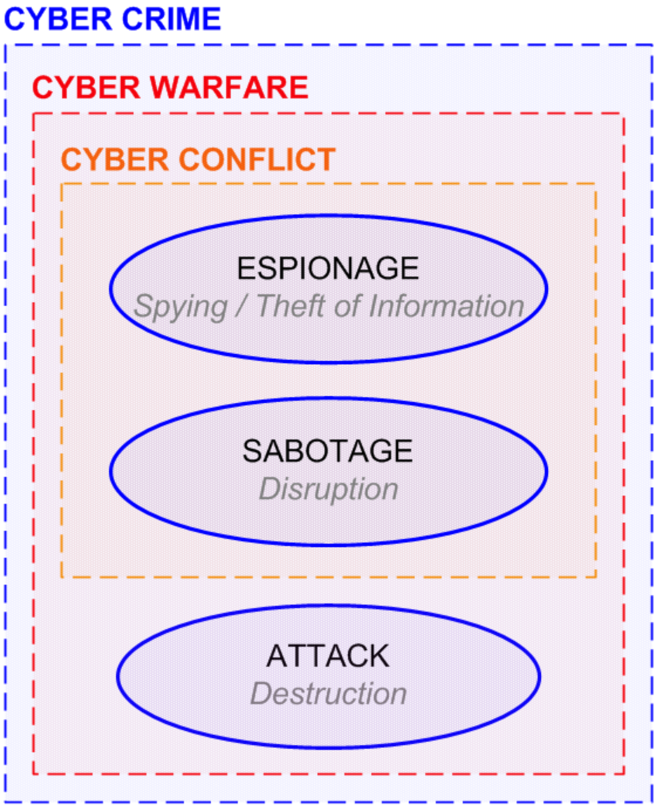

Figure 6. Subset relationship between Cyber Crime, Cyber Warfare, and Cyber Conflict

Cyberspace is a complex battle environment. In contrast to physical domains, in cyberspace, a risk accepted by one is a risk assumed by all. This becomes analogous to that of a chain only being as strong as its weakest link. The integration of networks has created a highly networked environment. This interconnection has allowed us to enjoy the benefits of an information technology revolution; however, the interdependence created between critical systems and networks has exposed major vulnerabilities.

Moving forward, more efficient, contained, secure solutions need to be developed, not to necessarily cut back on nodes, but to create interconnections intelligently - balancing security along with quality of service (QoS), similarly as Cisco adopting a three-tier hierarchical model comprising the core, distribution, and access layers for network design. Utilization of recent technologies such as thin-clients, virtualization, cloud computing, and VPNs should be considered whenever possible. In addition, boundaries need to be defined, as the perimeter layer within the DiD strategy is slowly being considered, by some, to be non-effective. Strategic questions need to be asked such as 'what happens if my workstation or routers if they become compromised?' and 'what does that do to my entire environment?' As interdependencies have spawned new vulnerabilities, proper and up-to-date documentation of network ingress and egress points becomes even more significant.

The industry must come together to address those vulnerabilities associated with SCADA systems. Although, the world is not headed in this direction, we must consider removing connectivity to critical infrastructures and control systems, belonging to private industries, off the internet. SCADA should not be on networks. A principle similar to that of USB thumb drives not allowed on military networks. The problem is that more and more designers of these control systems are embedding Ethernet jacks so that engineers can remote connect from home.

The interim solution is simple: take it off the network. However, in a global economy, commercial and private enterprises would argue that disconnections are not a strategic move for remaining competitive.

Privacy, civil liberties, and our freedom are the essence of what makes us Americans. We need to find ways of mitigating the risk to protect the nation in a way that is consistent with our values and laws. The problem is that the Internet was not originally designed to be secure. We need to foster solutions that will allow us to secure that which we've become so dependent on. One such way is through Cyber reform; using regulation to defend.

In the U.S. people have grown to communicate on the Internet anonymously. That is going to have to change. Online anonymity, or the ability to use the internet without identifying yourself, (privacy) should be considered a thing of the past. Cyber security can be implemented in a way that fosters accountability and non-repudiation, resulting in the widespread collection and disclosure of user information. New ways of establishing trust on the internet need to be developed - ways of establishing what can you trust between individuals, web servers, and companies. Depending on how much trust is required there this likely to be several levels of the Internet. For certain kinds of interaction you would need to know who you're dealing with and those not willing to verify their identity would simply be refused access.

Privacy advocates consider this kind of approach to security intrusive, claiming it threatens rights to privacy. However, is it really intrusive for the government to tell you to buckle up your seatbelt when driving? Might we simply be overacting? Eventually the Internet will need some form of regulation in order to curtail the increasing number of cyber-crime incidents by APTs, possibly preventing a cyber war in the future. Currently, the government can’t regulate the internet, leaving other concept solutions like bandwidth limitations for clients, and metered connectivity up in the air. To achieve the public confidence for regulations, a solution needs to be transparent, having public buy-in and support.

There are concerns that a 9-11 blueprint could resurface: a Patriot Act targeting cyberspace, citing how an intervention would be handled with civilian computers used as unwilling participants as part of a botnet attack. Would the client’s (Grandma’s) computer be considered a weapon? Privacy concerns could get chipped away under the guise of national security. The problem with botnets is that there are millions of computers with little to no security on them. Ultimately, public awareness and education about good security practices is what is needed in order to solve the botnet threat.

On April 27, 2012, the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA). If enacted, the bill would increase information sharing between the government and technology companies - a joint effort in the event of a cyber-security emergency - giving each protection to share information with one another to advert a cyber-attack. The government could share some classified information with private companies to help them protect their networks, and companies could share information about their users, and its networks with the government.

At the Pentagon, the U.S. military has classified cyber along with land, sea, air, and space as a domain of operations, to safeguard the integrity of our military’s critical information systems and infrastructures. It has been given its own command: U.S. Cyber Command (USCYBERCOM), with its own 4-star General, nominated by the President, to oversee the domain, while conducting both defense and offense against threats to the nation.

USCYBERCOM's Concept of Operations (CONOPS) defines three lines of operations for the command: DoD Global Information Grid (GIG) Operations (DGO); Defensive Cyber Operations (DCO); and engaging in Offensive Cyber Operations (OCO) (Friberg, 2011).

Further offensive cyber capabilities need to be developed (as in the case with Stuxnet). In so much as, like a game in sports, the only good defense is a good offense: the U.S. needs to be able to carry out offensive cyber-attacks to dissuade the enemy from attacking in the first place. Part of that is to have the capability to deter by responding, either by taking out the attacker or by being able to retaliate. Other capabilities include creating offensive opportunities, such as backdoor portable document files (.pdf), enacted if information falls into the wrong hands. Although, the key is not just the technology, but to define in terms of doctrine, what kinds of offensive steps we are willing to take, including those steps which are off limits; synchronizing legal with the doctrine.

While the U.S. very likely possesses the most sophisticated offensive cyber war capabilities, that offensive prowess cannot make up for the weaknesses in our defensive position (Clark, 2010). There are those who recognize that a much more defensive approach to defense needs to be taken. Addressing the predominate vector of attacks, coming from vulnerabilities existing on unpatched systems, and actual system administrators who are overworked, lacking adequate resources to complete their duties.

The development of the National Cyber Range will aid in the creation of an early cyber-attack warning system, including other capabilities, allowing DoD, other U.S. government entities, and potentially non-U.S. government partners to test and evaluate new cyberspace concepts, policies, and technologies. The National Cyber Range, which allows the rapid creation of numerous models of networks, is intended to enable the military and others to address these capability requirements by simulating and testing new technologies. (DoD, 2011).

Lastly, it is imperative that all commercial, private, and government agencies, responsible for national critical infrastructures, establish contingency plans to ensure that operations can continue. Contingency planning is the process of identifying the mission-critical functions of an organization that must be restored expeditiously during an operational disruption, disaster or malfunction. While the growing requirement for contingency planning has risen, many commercial and private organizations are not yet mandated to have these plans in place (Eiselstein, 1999).

Conclusion

Securing cyberspace is an extraordinary difficult strategic challenge that requires a coordinated and focused effort, not only from organizations throughout the DoD, but also from the federal, state, and local governments, and the private sector (US-CERT, 2003). With over 88,000 critical infrastructure assets identified by the DHS, cyber terrorists literally have a buffet of targets to pick and choose from. The era of cyber warfare has arrived with the likelihood of suffering a catastrophic cyber attack no longer considered abstract theory, but instead simply a matter of when such an attack will strike. The APT has already rapidly reached beyond our control, resulting in the extraction and loss of classified information, disrupting our defense and military networks. Cyber security and critical infrastructure protection have now become a matter of public safety and national security. The National Security Systems and supporting infrastructures that we rely on for water, power, transportation, communications, and emergency services are now under the threat of attack - attacks which have become increasingly difficult to detect and defend against.

Today, the implementation of current Defense in Depth (DiD) strategies is synonymous with just creating a higher wall to protect a castle. DiD strategies for national security systems and critical infrastructure protection must not only evolve to combat the rapidly growing number of cyber threats, but must also be offset with solutions, flexible enough to withstand the increased sophistication of new threats, including cyber weapons and the possibility of war within cyberspace.

Acknowledgements

Special acknowledgement is given to the following at United States Pacific Command (USPACOM) whose support and encouragement greatly contributed to the writing of this paper:

Mr. Randall Cieslak, SES	Chief Information Officer, USPACOM Information Systems Authorizing Official
Mr. Terry Scott, GS-15	Deputy Director for Communications, USPACOM
Col Douglas Mason, USMC	Division Chief for Communications, USPACOM
Ms. Leona Bangerter, GS-14	Deputy Division Chief for IT Services, USPACOM
Mr. Dunkin Walker, GS-14	C4 Strategy & Integration Branch Chief, USPACOM
Ms. Juliet Eiselstein, GS-14	Cyber Security Deputy Branch Chief, USPACOM Information Assurance Manager
Ms. Pamela Mitchell, GS-13	IA Governance Section Chief, USPACOM
Mr. Robert Mathieson, GS-13	CND Section Chief, USPACOM
Mr. Joshua Margolin, GS-13	C&A Section Chief, USPACOM

References

60-Day Review. (2009, May). Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. Retrieved May 30, 2012 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Cieslak, R. (2009, April). U.S. pacific command chief information officer guidance: Information assurance framework. United States Pacific Command.

Clark, R. (2010, April). Cyber war: the next threat to national security and what to do about it. HarperCollins Publishers, New York, NY.

CSIS. (2008, December). Securing cyberspace for the 44th presidency. Center for Strategic and International Studies. Washington, D.C. Retrieved May 30, 2012 from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

DHS. (2003, February). The national strategy for the physical protection of critical infrastructures and key assets. Retrieved May 30, 2012 from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

DoD. (2011, July). Department of defense strategy for operating in cyberspace. Retrieved May 30, 2012 from http://www.defense.gov/news/d20110714cyber.pdf

Eiselstein, J. (1999, March). Contingency planning—year 2000 solution. Bowie State University, Bowie, MD.

Friberg, H., Col (2011, February) U.S. cyber command to support geographic combatant commands. U.S. Army War College, Carlisle Barracks, PA. Retrieved

May 30, 2012 from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA543404

Mitchell, S. (2011, March). Stuxnet: anatomy of a computer virus. Retrieved May 30, 2012 from http://vimeo.com/25118844

NSA. (2001, June). Defense in depth a practical strategy for achieving information assurance in today's highly networked environments. Retrieved May 30, 2012 from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

NSPD-54/HSPD-23 (2008, January). The comprehensive national cybersecurity initiative. Retrieved May 30, 2012 from http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

PDD-63. (1998, May). Critical infrastructure protection. Retrieved May 30, 2012, from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

Robbins, P. (2011, December). Security risk analysis and critical information systems. Hawaii Pacific University, Honolulu, HI. Retrieved May 30, 2012 from http://dorkatron.com/docs/robbins.thesis.proper.pdf

Rosenquist, M. (2008, September). Defense in depth strategy optimizes security. Intel Corporation. Retrieved May 30, 2012 from http://www.intel.com/it/pdf/defense_in_depth_strategy_optimizes_security.pdf

US-CERT. (2003, February). The national strategy to secure cyberspace. Retrieved May 30, 2012 from http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf