CHAPTER

3

The Cyberspace Battlefield

INFORMATION IN THIS CHAPTER

- Boundaries in Cyber Warfare
- Where Cyber Fits in the War-fighting Domains
- Review of the Threat Actors
- Fielding Systems at the Speed of Need

The boundaries of the battlefield in the physical world are usually straightforward. When two countries go to war there is a battlefront established between the two armies where active combat occurs. While there is not a clear forward area to the battlefront for counterinsurgency, irregular warfare, counterterrorism, and foreign internal defense battles even there are two sides with political goals fighting over geography.

The chief challenge in dealing with this new virtual cyberspace paradigm is the separation of activities from geography. Reconnaissance can now be done by folks distributed across the world. Planning can be done by cells of combatants who never meet. The Internet provides a means of communications via secure channels. The Internet can be both a resource and an attack vector. This new battlespace is an intricate problem. To understand it we will look at the boundaries of this new battlespace, how it fits into the historical war-fighting domains, the enemy forces we are facing, and the weapons needed to win on this virtual front.

BOUNDARIES IN CYBER WARFARE

Upon examining the boundaries of this virtual battlespace, we see three areas to analyze: physical, logical, and organizational. In the physical world boundaries can be legally recognized (*de jure*) like the borders between countries or practical (*de facto*) like the division of terrain between two units in the same army; these definitions are more difficult to apply in the virtual world. If we think of the World Wide Web as a connection of smaller networks with different configuration rules it is easy to see where to divide it. For the U.S. government this

http://dx.doi.org/10.1016/B978-0-12-416672-1.00003-9

could be any system with .gov or .mil extensions which is the blend between the physical and logical. Generally each of these networks has a perimeter defended with a firewall, and anti-virus defending each machine. The more mature networks have a Security Operations Center (SOC) monitoring a Security Information and Event Management tool that includes feeds from Intrusion Detection Systems (IDS)/Intrusion Prevention Systems, correlation engines, web security proxies, centrally managed enterprise anti-virus/anti-spam servers, and forensics tools and compliance programs (ideally including training to help secure the users). These are the foundations for the defensive forces used in this battle. Finally there are organizations where a unit has multiple logical networks used by multiple groups (e.g., for a deployment to disaster relief) but also have multiple units that combine their networks to develop a single capability when they are part of a Joint or Multinational Command in an operational theater. This can present command and control challenges where physical presence does not line up with logical existence and the unit must coordinate action across many organizational boundaries to include government and commercial entities.

What do we mean by battlespace? The U.S. military definition is: "A term used to signify a unified military strategy to integrate and combine armed forces for the military theater of operations, including air, information, land, sea and space to achieve military goals. It includes the environment, factors and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes enemy and friendly armed forces; infrastructure; weather; terrain; and the electromagnetic spectrum within the operational areas and areas of interest" [1]. In cyber operations, battlespace includes things like the networks, computers, hardware (this includes weapon systems with embedded computer chips), software (commercial and government developed), applications (like command and control systems), protocols, mobile devices, and the people that run them.

Defense in Depth

In cybersecurity, Defense in Depth is designed to build a wall of protection around the network or throughout the battle space. It must be enhanced to protect against insider threats and mobile devices that migrate in and out of the perimeter. It is the standard practice for logical construction of a network. At the lowest level we have an individual home network behind a local Internet Service Provider (ISP) router, and at the other end of the spectrum we have a national state network like China behind their Great Firewall. The U.S. government is behind several hundred access points monitored by the Department of Homeland Security. Sub-groups like Department of Defense, Department of Energy, Department of State, and Department of Treasury, etc., all sit behind their own security infrastructure. Organizations maintain their own networks but use a variety of techniques to administer and secure them. Some build and maintain everything, others outsource the infrastructure but keep security in house, some outsource everything but have the equipment in their building, and finally some prefer cloud solutions. Many of these organizations are geographically dispersed with users in multiple locations across the world. The amount of protection they deploy is based on their perception of risk and willingness to invest their profit back into security for the network. When we look at their defenses it is based on economic power rather than military power.

NOTE

Cloud computing uses Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) to provide computing needs where the services are remote. Similar technology is Service Oriented Architecture (SOA) which is closely tied to web services. Both of these technologies often use Virtual Machines (VM) to host their systems on. These technologies provide benefits but come with new security issues to include data control, auditing, and configuration management. Like any system, they can be fraught with risk or very secure, based on how they are designed and maintained.

One concept that has been popular in the media is the concept of building a switch to isolate or "turn off the Internet" if we are under attack. These concepts show a fundamental lack of understanding of the Internet today. The Internet was a system originally built by Defense Advanced Research Projects Agency (DARPA) to provide communications capability after a nuclear war. As a result, it has resiliency and alternate path routing as part of the requirements. A good example of this can be seen in Iran's effort to suppress the protests following the 2009 presidential elections. Iran had government control over the communications systems and yet the Green Protest groups started a Twitter revolution using social media tools to get their message out (called the Twitter Revolution) [2]. We can quickly see that parts of the Internet can be turned dark, but only for a limited period of time and are actually a self-inflected denial of service.

Physical Infrastructure

Physical infrastructure includes power, backup generators, Heating Ventilating and Air Conditioning, surge control systems, connectivity (cabling), hardware, software, and people. The physical systems are vulnerable to surveillance, vandalism, sabotage, and attack. Much of this infrastructure is controlled by Industrial Control Systems (ICS), also commonly known as Supervisory Control and Data Acquisition (SCADA) programs which are vulnerable to hacking or denial of service attacks. Note that SCADA is a subset of ICS but has become synonymous in the media. This list does not address the potential environmental disaster factors. If the threat cannot conduct a kinetic attack or hack the system then there is always the wetware (human) vector. It is often easier to attack users than it is to attack the equipment. So when attacking the physical there are a number of options to create the desired impact.

NOTE

As with any subculture hackers have their own jargon. They use terms like: wetware for the human or user, noob or script kiddy meaning new or unskilled, PWN means to own, hacktivism is politically motivated hacking, and zombies/bots are systems that have been compromised and become part of a hackers network. There is also a unique way to write where letters and numbers are changed to make writing distinctive. Examples of this writing are elite becomes leet or 1337 or l33t and hacker becomes Haxor.

It is important to note that most of these infrastructure systems have systemic issues like: legacy systems, lack of lab environments to test patching, local management, and no SOC monitoring them. The programs are built on proprietary systems that originally ran on closed networks so were designed with high availability requirements but no confidentiality or integrity protections. SCADA owners believed that they would be protected by obscurity with nobody wanting to break into their systems. Also they felt that their programs were proprietary so would not be hackable, as the applications were unique. Most of these systems use the same protocols and are developed with the same programming languages as the rest of the applications on the market today so it has been relatively easy to find vulnerabilities in them. If we take a look at one critical infrastructure area like water, we have heard reports [3] about how terrorists could hack in and open dam gates to cause flooding or cause an infusion of the purification chemicals to the point where the water is toxic. The reality is cyber problems are competing with other issues with these systems. In many cases the cyber threats are not getting funding because fixing problems like repairing the dam gates to prevent maintenance failure, or cleaning the holding tanks that have toxic mold in them are a higher priority and consume all the funds that are available. Our infrastructure has many issues to be dealt with and cybersecurity is only a potential issue relative to the number of tangible issues they are facing today.

NOTE

U.S. Critical Infrastructure includes: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Information Technology, National Monuments and Icons, Nuclear Reactors, Materials and Waste, Postal and Shipping, Transportation Systems, and Water. Note that most of these are in the private sector and government control varies widely depending on the sector.

Organizational View

Organizations can be divided into commercial (including critical infrastructure) and government (generally divided into federal agencies and the military but there are hybrids like the Tennessee Valley Authority which have elements of both). These organizations all approach cybersecurity differently based on their risk tolerance, regulations, and resources. Commercial companies are market-driven and must spend just enough on security to manage risk appropriately. These companies must make decisions based on Return on Investment (ROI) which leads to the eternal struggle between the Chief Financial Officer (CFO) and the Chief Information Officer (CIO). Today many CIOs calculate Return on Security Investment using formulas like Annualized Loss Expectancy (Vulnerability $\times$ Threat $\times$ Asset Value = Total Risk then Total Risk $\times$ Countermeasures = Residual Risk). This translates into the following sample scenario: the chance of getting a virus attack is 100% (in fact expect one a day), the cost of which is three hours of lost productivity and one hour of IT support times total number of employees (200) leads to the following equation—365 viruses $\times$ \$450 labor $\times$ 200 people = \$3,285,000, which indicates that a company is better off buying anti-virus at \$40 per system for total of \$8000 to reduce risk to an acceptable level. With the need for cost

saving in the government, these types of calculations are becoming more common in the military today.

Companies also pull in the legal team to review what their due care/diligence responsibilities are in case they are sued. For example, if they were to lose customer privacy data, they might be sued. This evaluation is based on what a reasonable person would expect them to do to protect their information. The size and resources of the company play a big role in determining what "best practices" they should be following for their industry. Finally, depending on which market sector we are talking about, ROI could mean Risk of Incarceration based on laws like Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach-Bliley Act of 1999, or Sarbanes-Oxley (SOX) Act of 2002. One comparison many security professionals make is the amount spent on physical security and property insurance versus what is spent in Information Assurance versus their relative value to the success of the company. There is a balance between budget and level of risk. Some CIOs spread Fear, Uncertainty and Doubt to get their budget approved, rather than work the numbers, which has given the IT Security Industry a bad reputation. The simple fact is that today if a security team was given an unlimited budget they could not guarantee that there would not be any intrusions because there are constantly new vulnerabilities. Some CFOs feel it is a waste of money to do more than the minimum security protection measures. They point to examples such as when T. J. Maxx and Heartland were in the news for being hacked but they still made a profit the next quarter. There is a reasonable level of security that should be implemented based on which industry the company is in (i.e., financial institutions would spend more than manufacturing) and what risk the leadership is willing to take. The key is making sure the leadership understands the risk that they are accepting in this contested virtual economic battlefield.

Next we have the federal government, which has dispersed responsibility throughout the different agencies who all use different tools and processes. Most cybersecurity is based on compliance with regulations like National Institute of Standards & Technology (NIST) 800-XX series, the Federal Information Security Management Act (FISMA) of 2002, or Homeland Security/Presidential Directives. The White House has a cybersecurity coordinator but the major player is the Department of Homeland Security (DHS). The DHS controls the U.S. Computer Emergency Response Team, National Incident Response Plan, Critical Infrastructure Protection Plan, and the Einstein IDS program.

The Federal Bureau of Investigation (FBI) has a Cyber Division, the InfraGard outreach program, the Internet Crime Complaint Center, and the National Cyber Crimes Investigative Joint Task Force that add up to some impressive forensics capabilities. Their focus is domestic crime and counterterrorism not cyber war, but they have some useful tools and processes to help fight the cyber war. One major success the FBI had was the Darkmarket sting, when they took down a major identify theft ring [4]. They continue to get better at conducting computer investigations internationally [5] with 61 legal attaché offices around the world conducting joint investigations with countries like Romania, Estonia, Ukraine, and the Netherlands.

Another agency that is moving into the digital battlefield is the Federal Aviation Administration (FAA) with the Next Generation Air Transportation System (NextGen) project to move from analog to digital systems to provide safer, more convenient, and more dependable travel. As with any system, as it moves to the network it increases accessibility which also opens a new set of attack vectors.

The Department of Energy is becoming a major cyber player with Smart Grid and energy grid security. With the potential for everyone's appliances, heating/air-conditioning, entertainment systems, and home security systems being put online they are opening up a new field for the hackers to move into. DoE is working to build security into the smart grid but it is very complex. They have done some great work in their National Labs like Sandia National Laboratory and Idaho National Laboratory, to name two of the seven labs working on cyber solutions.

Finally, the Department of Justice (DoJ) must decide which cases to take to court and sets the tone for what is acceptable behavior by deciding where to put their prosecution resources. Today, the DoJ is focused on terrorism and drugs rather than hacking or cyber war incidents.

On the military side, the DoD has a very complex hierarchical authority structure. Despite standing up US CYBERCOMMAND, the individual services (Army, Air Force, Navy, and Marines) still have the authority and budget to decide how to implement cybersecurity. Each branch of the service has a name for their portion of the network. Defense Information Systems Agency (DISA) runs the Global Information Grid (GIG), the Air Force has C2 Constellation, the Army has LandWarNet, and Navy has FORCEnet. The emerging initiatives to transform network capabilities are Joint Information Environment (JIE), DoD Enterprise Portal Service, Enterprise Cloud Broker, and standardize mobility solutions. These are not formal programs of record but rather efforts to respond to new budget constraints and capability demands. There are also different levels of classification on information and networks. The DoD uses Unclassified, For Official Use Only (FOUO) or Controlled Unclassified Information (CUI) or Confidential, Secret, Top Secret, Sensitive Compartmented Information and Special-Access Program/Special Access Required (SAP/SAR). The associated networks are Non-Secure Internet Protocol Router (NIPR) for unclassified, Secure Internet Protocol Router (SIPR) for Secret and Joint Worldwide Intelligence Communications System (JWICS) for Top Secret. In addition, there are separate networks like the Defense Research and Engineering Network (DREN) for research. Finally, deployed forces build their own networks in theater that connect to many of these "reach back" networks as well as to fellow coalition nations via multinational forces networks. An example is if a unit from Fort Carson deployed to Afghanistan has to build a network in country or theater, they would want to connect back to resources at Fort Carson and to other international forces they are teamed with. It is not unusual to see a Tactical Operation Center (TOC) with 6-12 terminals representing the different networks. It is easy to see that there is not a clear chain of command for the network of networks supporting DoD.

As important as these networks are, they do not include the full scope of the modern virtual battlefield. Today command and control of forces is done digitally, weapon systems are connected to the network and depend heavily on computing power, intelligence dominance is key to our ability to wining on the modern battlefield, and it is completely dependent on computer applications/systems. For example in 2006 during a military simulation for an Air Operation Center (AOC), a young airman was asked what would happen if the network went down. He said they would have to stop flying missions. That is, of course, untrue as leaders of the pre-digital generation were flying similar missions long before computers were used for command and control and there are continuity of operation plans in place in the event that the network goes down; but the younger generation's perception and dependence on the network was astonishing. Note that the loss of the AOC's network would have a huge impact

on the ability to process orders nearly as fast or accurately as the current "information dominance" systems allow but it would not stop them.

When we talk about CYBERCOM and the Services (Army, Navy, Air Force, and Marines) it is important to remember that the Services train and equip the forces and the Combatant Commanders call on the services to provide forces for their missions. Strategic Command (STRATCOM) has the mission to "ensure U.S. freedom of action in space and cyberspace" [6]. Cyber Command's (CYBERCOM) mission is to "plan, coordinate, integrate, synchronize, and conduct activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries" [6]. Each Service has a Cyber Unit that supports CYBERCOM, the Air Force has the 24th Number Air Force, the Army has Army Cyber Command (ARCYBER) or 2nd Army, the Navy has the 10th Fleet, and the Marines have Marine Forces Cyber. Closely aligned to these forces is the Intelligence Community, specifically the National Security Agency. This results in different priorities and authorities based on the different mission each organization has.

It is important to note that there are U.S. codes that set the rules for how these units operate. There are a number of titles that provide specific guidance. Title 10 is Armed Forces and is the law that regulates how war is fought [1]. Title 50 is War and National Defense and generally covers intelligence and counter intelligence [1]. It is interesting to note that some units had their authorized mission changed from being under Title 50 to Title 10 as part of the CYBERCOM stand up. Title 18 is Crimes and Criminal Procedure, which covers taking the attacking party to court [1]. Many people are now talking about the need to merge these three into one integrated process (sometimes called title 78). Other titles often used are Title 32, which is National Guard and Title 14 which is the Coast Guard [1]. These forces are not as restricted by laws like Posse Comitatus, which restricts the federal government use of the military for law enforcement. Today we see Joint Operation Centers with forces from multiple "title source" or "forces" to allow them to operate effectively based on the different rules they must comply with.

So we see the commercial sector is driven by the market, the federal agencies are all driven by their function and compliance requirements, and the military is driven by mission and the regulations they have to operate under, and everyone must deal with a limited budget! All of them are facing the similar threats and vulnerabilities. There are efforts to coordinate between them but there is no central authority to drive integration; again each organization is doing their best based on their mission and resources. So let us take a look at the domain we are talking about.

WHERE CYBER FITS IN THE WAR-FIGHTING DOMAINS

Cyber is ubiquitous throughout Land, Sea, Air and Space. Initially there were only two war-fighting domains: land and sea. Land is the area where combatants fought. Over time there were developments in weapons that would give one side or the other an advantage but they would face each other on the field of battle. Then the sea became both a separate war-fighting domain and a part of supporting the land domain fight. The Maritime domain [7]

includes the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. Sea forces supporting a land force, usually with artillery fire, is known as littoral battle. Littoral support has two operational environments: Seaward, the area from the open ocean to the shore, which must be controlled to support operations ashore, and Landward, the area inland from the shore that can be supported and defended directly from the sea. Ships would fight battles to both control the sea and support land battles. As technology continued to influence the battlefield, airplanes were introduced. The air domain is the defined as "within the earth's atmosphere"; beginning at the Earth's surface and extending to the altitude where its effects upon operations become negligible [7]. The first airplanes were used for reconnaissance but were soon armed and fought both air-to-air and air-to-ground engagements. Then warfare reached space. Space is the environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere [8]. This was a unique domain as it was used by the other domains rather than a domain where combat was fought (though at some point it will become another battlefront). Finally Cyberspace became so vital to the war-fighters it was declared a domain. It is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [8]. Modern commanders depend on it and are actively studying how to fight and win the next war on it. Next we will take a look at each of the first four domains (land, sea, air, space), and see how they relate to cyber.

Land Domain

As we look back at the progression of warfare on land we see there have been many Revolutions of Military Affairs (RMA). The rock gave way to the club, which was beat out by the spear and then the bow. Horse-mounted soldiers had an advantage over ground troops and then the stirrup gave them a tremendous advantage. Guns and artillery increased the rate at which armies could kill each other as well as the effective range at which they could kill. Next came the tank and machine guns. Each of these RMAs changed how armies organized and fought. New doctrine, tactics, and organizational structures had to be developed. Should we integrate the new weapons into every unit or build a unit of pure machine guns/tanks? The decision was tank units should consist of tanks by themselves but the machine gun should be integrated into every unit. The decision to make tank units of pure tanks has been reversed. Today, the tank is normally integrated with infantry to form "combined arms task forces" so the commander can leverage each unit's strengths. These historical lessons in transformation must be studied to find how to most efficiently develop methods of fighting in this latest RMA—cyberspace.

Sea Domain

In many ways the sea is an analogous battlefield to cyberspace. Similar to cyberspace it is a large area where ships can easily move without detection so the defender has the challenge of

detecting where the threat is. No one side can control it. The criminal elements operating on the Internet are comparable to the pirates of old who would interdict and influence the lines of commerce. There were eventually international agreements developed to deal with these threats. Another example we can draw from the Navy is the development of the Flattop or Aircraft Carrier. For years the battleship was the measure of a nation's sea power but the introduction of the Flattop caused a paradigm shift and soon strategies, doctrine and tactics were built around it. Most senior officers had built their careers around the battleship and the defense industrial base was heavily investing in the battleship so they strongly resisted the transformation. They refused to see the need to change based on a new capability. This cultural blindness is impacting the transformation to computer network operations in many of today's organizations. At the tactical level many security professionals still base their strategies on outdated technologies, even though the industry and the battlespace have transformed and evolved. They are still focused on perimeter defenses and ignore the mobile devices being used by their workforce. At the senior leadership level the lack of understanding of the technology and its implications in some organizations impedes the development of doctrine to fight the next war.

Nowadays we have commanders who have grown up with the idea that weapon systems must be based on their ability to put "steel on target," and that the idea of a weapon system that does not destroy something via kinetic attack is ridiculous. They also do not feel that their "real" weapon systems (e.g., jets or tanks) should be considered part of the virtual battlefield because they are enabled with computer chips (despite the fact that they can be hacked into and modified). Some still believe that non-kinetic attacks are something that would only be an annoyance (like their email going down) or play a support role—not be part of a battlefield engagement strategy. These are the same professionals that study history and understand transformation but struggle to understand the technology running the systems they depend on. It is a challenge because they are steeped in tradition and have studied warfare based on the weapons that existed when they were junior officers and still in the field. It is a constant struggle to understand the changes that technology is bringing to the battlefield.

Air Domain

Airpower is similar to cyber power because it is a domain dominated by technological advancements. Early on there were major leaders developing strategies, doctrine, and tactics. General Giulio Douhet was an Italian officer who was one of the first real theorists supporting the use of Air Power [9]. He felt that there was no defense against bombers: it would terrorize populations into surrender. He advocated the use of explosive, incendiary and poison gas bombs against population centers as he felt the entire workforce contributes to the total war effort making everyone a legitimate target. General Douhet was court-martialed for his outspoken beliefs.

Billy Mitchell is considered the father of American Air Power. He came into World War I as a lieutenant colonel in the Army and ended up controlling all U.S. air forces [10]. He is a controversial figure because of the disagreements he had with the Army leadership over using air power against battleships and was court-martialed for insubordination. His passion for how air power could be used was key to the development of Air Force capabilities. Both these

general officers understood the potential for air power and pushed for innovation at the expense of their careers, both eventually had their court-martials overturned and are considered heroes. We have not seen anyone with that level of forward thinking theories and dedication for cyber warfare in today's military.

Space Domain

Space is very comparable to cyberspace in that it is generally considered an enabler to the other domains. It provides communications paths for most long-haul communications systems, Command and Control (C2), Intelligence Surveillance and Reconnaissance, navigation based on Global Positioning System, phones, radios, television, financial transactions, and surveillance for wide area reconnaissance, weather, mapping and commercial imaging (i.e., Google maps). The George C. Marshall Institute produced a great series called "A Day without Space" which lays out all the impacts. Space provides some great examples on how to integrate a new technology into the armed forces. Space started as a military dominated domain that has transitioned to a commercial market just like cyber operations. It is a technology that integrated into the other domains to the point they are dependent on it. It is an area that requires unique skills so the management of the workforce presents a challenge. It takes time to build senior leaders for a new technology and as the commercial demand takes off the competition for the workforce gets fierce. It is very hard to retain skilled operators in cyber and space-related fields.

Cyber Domain

Cyber is ubiquitous in all the other modern domains. In 2010 Lt. Gen. William T. Lord, Air Force chief of war-fighting information said "I think that a day without cyber brings you back to about World War I days" [11]. When we talk about the cyber domain some will say it is limited to the hardware that runs the military networks (e.g., computers, routers, firewalls), others will say it is the military networks and the supporting infrastructure (e.g., defense contractors and long-haul communications providers), a few believe it is all government systems, still others feel it is all systems connected to the Internet (all private and government systems). As we look for precedents we can see maritime law could be used, or international space treaties could apply or maybe we could develop a cyber manifest destiny. Some of the answers are overly simple or fit within current legal rules but ignore the reality of how interconnected these systems are. The problem is complex and, much like defining the boundaries in an insurgency conflict, may require different answers for different audiences. This domain is in need of theorists, strategies, doctrine, and tactics that shape what the domain and cyber war itself is scoped to include and exclude.

Combined Arms

While we have talked about the domains as separate and distinct the military integrates them for maximum effect when conducting combat operations. Different branches of the military integrate to achieve force multipliers, for example an infantry brigade would have an armor platoon attached to each battalion, be supported by an artillery unit and close air

support from the Air Force, have air defense to protect them from enemy aircraft and engineers to clear obstacles. In other scenarios the Navy, Space or Special Forces could be part of the force design. Now cyber must be both a domain to operation in and force to integrate.

REVIEW OF THE THREAT ACTORS

No analysis of war can be done without a thorough understanding of the enemy forces and their composition, disposition, strength, centers of gravity, and terrain. You will find this was true under Sun Tzu, Napoleon Bonaparte, Alexander the Great, and still today. We will look at the type of forces active in this battlespace, what impacts they are causing and what their motivations are. Understanding that these forces change quickly and they do not follow any set strategies, doctrine, or tactics we will categorize them by their actions.

NOTE

Center of gravity is the source of power that provides moral or physical strength, freedom of action, or will to act [12]. The center of gravity could be military forces or the will of the people to support the war. In cyber warfare, for a nation that bases its ability to win wars on information dominance, it could be their ability to collect, analyze, and act on data.

Most Active Threats

Let us get into the threat spectrum as seen in Figure 3.1. This is a different way to look at the information from Chapter 2 on Threatscape. There are a lot of folks out there trying to be "hackers." Most of them are what we call script kiddies. These are folks who just go out and grab tools off the Internet and try to break into systems. They are also known as noobs (as in newbies) because they are new to hacking and will generally only get the low-hanging fruit like unprotected home systems. Next come criminals. As soon as we started shopping and banking online the criminals saw the money and quickly followed to take advantage of the new opportunity. Many of these are professional organizations. If someone graduates with a degree in computer science in many poor countries the best paying jobs are with organized criminal gangs. The most famous is out of Russia and is known for the ISP they use called the Russian Business Network. Now they have well-educated people working 40-60 h a week trying to break into a specific target (i.e., Chase Bank or Ford for the latest designs). If they develop a zero day exploit it will only be used against that one company until the job is complete.

FIGURE 3.1 Ranking of different threats on the Internet.

Next we have hacker groups like the classic "Cult of the Dead Cow" who released a tool called "back orifice" at one of the more famous hacker conventions, DEFCON, starting back in 1998. These groups develop powerful tools but the Anti-Virus (AV) and IDS companies quickly analyze and post protections against them. Possibly the most dangerous group is the malicious insider. Typically, it is estimated that they represent 20% of the threat but cause 80% of the damage. Though studies like the annual Computer Security Institute (CSI) report show that number is growing [13]. Typically, we group insiders as disgruntled, or seeking financial gain. It is often hard to detect them as they are authorized users so we must look for unauthorized behaviors when most of the security today is on the perimeter looking for someone breaking in. Political/Religious groups practice recruitment, influence operations, and often attack the opposing viewpoint's websites or networks (commonly called Hacktivism).

Finally comes state-controlled or -sponsored groups, which have become known as the Advanced Persistent Threat (APT). These can be military units or loosely affiliated groups who may receive direct or indirect support from the government. The one we see in the news most today is China, which has been accused of systematically stealing information from both the military and the defense contractor base. However, there are many countries engaged in these activities. Some nations have devoted significant resources to these capabilities and we can only surmise their level of activities and capabilities.

Most Dangerous Threats

Now as we look at the impacts or damage the threat can cause, we see a very different order. It is important to measure out incidents based on the impact they have, rather than the amount of activity it caused. It would be easy to say that the slammer worm had a significant level of activity and compromised a large number of systems but when we consider that it had no payload to cause damage to our information it suddenly becomes only a nuisance. At the same time a spear phishing attack that successfully compromises the CEO of a Fortune 500 company would be an insignificant technical event but could cost the company millions. It is not the volume but the impact we need to measure, and to do that we must understand the criticality of the data on our systems.

If we sort the threats by the amount of damage caused, the order is APT/nation state, insider threat, terrorism, physical/environmental events, criminal attacks, hacker groups, unintentional, hacktivism, and Noob/Script Kiddy attacks (as seen in Figure 3.2).

FIGURE 3.2 Ranking of level of impact different threats can have.

Today APT is stealing billions of dollars worth of intellectual property and sensitive military information. One of the most widely reported military incidents was the F-35, "Computer spies have broken into the Pentagon's $300 billion Joint Strike Fighter project—the Defense Department's costliest weapons program ever—according to current and former government officials familiar with the attacks" [14]. Looking at commercial incidents it would have to be the Aurora incident involving Google, mentioned in Chapter 1. These activities are conducted daily by many different countries. Though some say it is only espionage or spying, a better description would be a full-scale economic war.

Next on our list is the insider threat. It can be damaging in many ways. Some insiders embezzle funds or take valuable information with them, or even leave malicious code like a logic bomb behind to destroy information after they are gone. Or they could bring illegally stolen information into our company when they are hired and expose the new company to lawsuits.

As we look at terrorism, it is doubtful that a terrorist would conduct a purely cyber attack when they could use it to increase the impact of a physical attack by causing a denial of service attack against emergency phone services, police surveillance systems, and traffic control systems.

Physical and environmental attacks can be both natural and man-made. A simple backhoe could isolate large portions of a network, turning on the fire sprinkler system could flood the server room, and heat from a fire or from taking out the air-conditioning can wipe out a server room. There are a number of ways to use attacks against facilities to cause a cyber impact but these are generally very localized.

Criminal attacks are causing a steadily increasing level of pain. It is becoming a national security concern as the general population is losing trust in conducting commerce over the Internet. Identity theft is now a household word, every scam and con has been converted for use over the Internet, and both individuals and banks are losing millions every year [15]. Anyone can buy stolen credit cards, malicious viruses, and botnet armies on the Internet (though it is hard to find reputable vendors). These can all be used as resources for cyber war if that is the intent.

Hacker groups are still around but have become more mainstream. They now have podcasts and attend hacker conventions. They still release new hacker tools and vulnerabilities but they are often shared with the security community before they are shared with the public.

Unintentional actions are often as painful as the attacks, with user actions, patches, configuration changes, and loading new services that cause denial of service and loss of data. These can be mitigated through training, testing, and backups but few organizations have the resources to do these correctly.

Hacktivism sounds exciting and we have had events like the one in 2001 that caused the first major "hacker conflict" when a U.S. spy plane was forced to land in China. "As China and the United States attempt to peacefully end their diplomatic standoff sparked by the mid-air collision between a U.S. spy plane and a Chinese fighter jet, crackers from both countries continue to wage private wars on the Internet" [16]. There were a lot of attacks from both sides and no prosecution on either side but it made for great media coverage. We can see this kind of activity between citizens of different countries or between political parties in the same

country. The concern from a cyber war point of view is we now have multiple factions joining the virtual battlefield. It is like watching a soccer game with the fans able to walk around on the field during play.

Finally we have the Noobs or Script Kiddies, who are the hackers that will grab well-known tools and just attack systems. They have little to no understanding of the hacker methodology (addressed in Chapter 6) or techniques to break into systems once the tool they are using does not work. Their biggest impact is they cause so much data or noise that it makes it very difficult to find the truly dangerous threats.

WARNING

It is odd that most companies today spend the same amount of money on protection of all their systems. Let us say someone spends $1M USD a year and they have 100K systems. That is $10 per system; now do all 100K systems have the same kind of info? No, some have no critical or mission-essential data and others hold the keys to all the corporate proprietary information. Yet we protect them all the same. This is one area where the economic war should force us to invest in Return on Security Investments by carefully categorizing our data based on its value and protecting it accordingly.

Motivations

Hacker's motives are varied but generally are ranked by amount of activity in this order: Money, Espionage, Skills for employment, Fame, Entertainment, Hacktivism, Terrorism and War (as seen in Figure 3.3). Most hackers are motivated by money; whether they are considered criminals or not depends on the country in which they live. Next comes the nation state or corporate espionage to gain some military or economic advantage. This is an area where it is often cheaper and more efficient to conduct cyber operations than use traditional spies. There is a high demand for these skills and many individuals are getting into the field because it is a hot job market but most do not have both a cyber and intelligence background. There is a lot of debate on whether it is smart to hire a "hacker" but just like some banks hire ex-cons to evaluate their security many network managers think we need to hire someone who thinks like the enemy to beat them.

FIGURE 3.3 Ranking of the motivations for the threats.

TIP

There is no governing body for computer security so we have no professional standards or definitions. Here are some quick and easy definitions we have come up with:

- Event—any recorded/logged activity (no logging = no events)
- Incident—any event we investigate (some turn out to be nothing = false positive)
- Intrusion—any compromise of a system (ranging from a virus to a person breaking into a system – most organizations break out 5-10 categories of intrusion, based on the severity of the compromise)
- Virus—malicious code that requires interaction to spread/execute (i.e., open a PowerPoint that has a script embedded that installs a program to compromise the system)
- Worm—malicious code that spreads/executes on its own (executes a vulnerability then compromises the system and uses the system to attack other systems)
- Trojan Horse—malicious code that masquerades as legitimate code (virus that is named a legitimate operating system file)
- Backdoor—code or configurations that allow access in the future (keep a port open and listening to allow the hacker to connect anytime they want)
- Rootkit—malware that compromises the brain of the operating system (called the kernel) so our system tells us what the malware wants us to see rather than what is really happening (lying about what files, processes, or programs are really running)
- Phishing—efforts to steal our identity or access credentials (usually via email)
- Pharming—efforts to steal mass groups worth of identity (usually compromise the database with all the financial information)
- Spear Phishing—effort to steal a specific VIP's identity (target a general officer or a chief level executive in a company)
- Zombies—systems on a network that are controlled by a hacker
- Botnets—group of networked systems controlled by hacker
- Honeynet/Honeypot—system whose sole purpose is to be compromised (allows security professionals chance to analyze the malware)

The days when system administrators saw a spike in the number of attacks during the summer and on spring break are long gone, but there are still individuals out there hacking for the challenge, entertainment value, or seeking fame. Others see it as a way to promote their beliefs through attacking the opposition, or simple vandalism of their web sites. The smallest groups are sometimes the most dangerous as they can concentrate skills and minimize exposure. There are organizations and countries that are developing the plans and capabilities to use the World Wide Web (WWW) to cause or increase the impact of terrorism and even full-scale wars.

FIELDING SYSTEMS AT THE SPEED OF NEED

One of the challenges facing most programs today is that there are no security requirements designed into the systems being built. A number of systems that are fielded today

never have security designed in, so security has to be bolted on after they are fielded. This results in both weaker security and higher costs.

Another challenge is the time it takes to field a new system. In 2009 Deputy Secretary of Defense William J. Lynn, III said "A more nimble IT acquisition process is even more important with the transition away from supplemental appropriations bills which had allowed us to deliver crucial war-fighting technologies outside the usual budget acquisition processes. As we return to funding wartime programs through the base budget, we need to build greater responsiveness in our standing processes. We need to redirect IT systems from an 81-month march to obsolescence and put them on a path to meet war fighters' evolving needs" [17]. We need to change the acquisition system to move at "the speed of need." This does not mean fielding systems that have not been through testing but rather making sure we do the testing in a cost-efficient and rapid manner.

Moore's law demands that we keep our capabilities inside an 18-month window. For cyber attack weapons the shelf life could be weeks depending on who else discovers the vulnerability or if normal patching fixes it. The generation coming into junior leadership positions has grown up with technology and wants the same capabilities they have at home in the workplace and are not satisfied hearing that every device has to go through an evaluation process that could take a year before it can be used in a secure facility. In the commercial sector we are hearing that the employee is always right today and the IT department needs to give them the tools they want to get their job done. So there are a number of factors driving rapid deployment but they lead to a history of security issues. It was difficult to get security right when the process was methodical so how do we expect to build a secure network with a reduced acquisition cycle? The answer is focusing on risk management and understanding when and where to take risks. We need to spend less time analyzing the device and more time monitoring it. We also need to understand that this domain will always be in flux and our systems cannot always be secure but they can be well managed and monitored.

As we look at how government contracts involving cyber operations are done today we see some trends. Overworked contracting offices have little experience with cybersecurity so they are challenged to address it in the requirements sections of the contracts they are developing. Most contracts for IT services have cybersecurity embedded as part of the overall task list, but it is not a critical evaluation criteria. Many Program Managers think the first place you can cut cost is by dropping security capabilities because there is no perceived loss of functionality to the system. The pain of these cuts are not felt until there is a public cybersecurity incident and the users must demand a redesigned secure system. A few contracts are pure cyber contracts that require quantifiable criteria for selection but the criterion are not very mature as this is a relatively new field. These contracts are normally for monitoring or validating the security of the network. The advantage of these contracts is that we are just measuring the security capabilities so we will not end up with a strong overall program that has a weak security subsection. This also keeps the funding and management separate so security does not get subjected to other network concerns. In a cyber conflict it is vital to have the security team be independent.

Most contract requirements are driven by regulations not risk management. In the cyber field these come from compliance rules and regulations. There is the NIST 800-XX series, North American Electric Reliability Council (NERC) has issued eight reliability standards on cybersecurity, DoD Information Assurance Certification and Accreditation Process

(DIACAP), and the Intelligence Community uses Director of Central Intelligence Directive (DCID) 6/3. There are laws and international agreements. There are commercial standards like International Organization for Standardization (ISO) and Information Technology Infrastructure Library (ITIL). All of these provide a starting point to develop standards for performance on contracts.

SUMMARY

We have studied the boundaries of cyber warfare and examined the many different perspectives that are used to define it (logical, physical, and organizational). These all have complexities that end up causing multiple strategies and solutions to be used.

We studied the traditional war-fighting domains of land, sea, air, and space both as they relate to cyber operations and what we can learn from them as we develop cyber as a war-fighting domain.

We reviewed the different threats (most active to least active: Script Kiddies, Criminals, Hacker Groups, Insiders, Political/Religious, APT/Nation State), the impact they have (high level of impact to low level of impact: APT/Nation State, Insider Threat, Terrorism, Physical/Environmental Events, Criminal Attacks, Hacker Groups, Unintentional, Hacktivism, Noob), and their motivations are (most common to least common: Money, Espionage, Skills for Employment, Fame, Entertainment, Hacktivism, Terrorism and War).

Finally, we examined how acquisition is enabling and fettering cybersecurity. All of these areas are immature and in need of policy, law, doctrine, tactics and education to ensure that if the next war is in or employs cyberspace we are ready.

References

[1] Congress. US house, http://uscode.house.gov/; 2010 [accessed 17.03.13].
[2] Leyne J. BBC news. How Iran's political battle is fought in cyberspace, http://news.bbc.co.uk/2/hi/8505645.stm; 2010 [accessed 17.03.13].
[3] FBI, Testimony of Ronald L. Dick, director, National infrastructure protection center, congressional testimony, http://www.fbi.gov/news/testimony/testimony; 2010 [accessed 17.03.13].
[4] FBI. Headline archives, http://www.fbi.gov/page2/may09/cyber050509.html; 2010 [accessed 17.03.13].
[5] FBI. Headline news, http://www.fbi.gov/page2/oct08/darkmarket_102008.html; 2010 [accessed 17.03.13].
[6] DoD. STRATCOM. Strategic command, http://www.stratcom.mil/; 2010 [accessed 17.03.13].
[7] DoD. Joint electronic library, http://www.dtic.mil/doctrine/; 2010 [accessed 17.03.13].
[8] DoD. Dictionary of military and associated terms, http://www.dtic.mil/doctrine/dod_dictionary/index.html; 2010 [accessed 17.03.13].
[9] Air force historical studies page. Out of print, http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf; 2010 [accessed 17.03.13].
[10] Museum, Maxwell Air Museum. Air chronicles, http://www.airpower.maxwell.af.mil/airchronicles/cc/mitch.html; 2010 [accessed 17.03.13].
[11] Grant R. Battling the phantom menance. Airforce-magazine.com, http://www.airforce-magazine.com/MagazineArchive/Pages/2010/April%202010/0410menace.aspx [accessed 17.03.13].
[12] DoD. Dictionary of military and associated terms, http://www.dtic.mil/doctrine/; 2010 [accessed 17.03.13].
[13] Computer Security Institute. CSI computer crime and security survey 2009, http://gocsi.com/; 2010 [accessed 17.03.13].

[14] Gorman S, Cole A, Dreazen, Y. Wall Street J Tech 2009, http://online.wsj.com/article/SB124027491029837401.html; 2010 [accessed 17.03.13].
[15] IC32009 annual report on internet crime released, http://www.ic3.gov/media/2010/100312.aspx; 2010 [accessed 17.03.13].
[16] Delio M. Crackers expand private war. Wired, http://www.wired.com/politics/law/news/2001/04/43134; 2001 [accessed 17.03.13].
[17] Defense, Department of Defense. Office of the assistant secretary of defense (Public Affairs). Speech, http://www.defense.gov/speeches/speech.aspx?speechid=1399; 2010 [accessed 17.03.13].