SYNGRESS

Cyber Warfare

Techniques, Tactics and Tools for Security Practitioners

Second Edition

Foreword by Stephen Northcutt

Jason Andress

Steve Winterfeld

CHAPTER

1

What is Cyber Warfare?

INFORMATION IN THIS CHAPTER

- What is Cyber Warfare?
- Have We Seen a Cyber War?
- Why Cyber Warfare is Important

We are constantly bombarded with news about cyber events today. There are constant headlines: *cybercrime is up, watch out for the latest phishing attack trying to steal our identity, update our antivirus to avoid infection, patch the operating system to avoid a hacker taking control, new zero day attack against smartphones, Facebook privacy compromised, someone took down Twitter*, and now we cannot go for more than a week without hearing about cyber war.

When establishing the boundaries of the battlefield in the physical world it is usually straightforward. When two countries go to war there is a battlefront established between the two armies where active combat occurs. Wars have traditionally been fought over land, and typically on the very land the countries are fighting for but in the current war on terrorism, the reasons and boundaries are less defined, with no set battlefront where the forces clash, and distributed forces conducting guerrilla or asymmetric warfare with no formal rank structure or doctrine.

Still, even in unconventional warfare the two sides operate within the same geographical area; in cyberspace the traditional physical boundaries disappear.

WHAT IS CYBER WARFARE?

Background

We have been reading about cyber acts of aggression for years now. Cliff Stoll first published *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* in 1989 about Soviet Bloc countries breaking into Department of Defense (DoD) sponsored networks. Seven years later we see a very similar storyline from both sides of the hack in

Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It by Tsutomu Shimomura and John Markoff with its opposing view in the book *The Fugitive Game: Online with Kevin Mitnick* by Jonathan Littman. Today we see a host of books on crime, hacking, defensive practices, and certification prep guides not to mention cyber plots in fiction books like *The Blue Nowhere* by Jeffrey Deaver, *Debt of Honor* by Tom Clancy, or *The Scorpion's Gate* by Richard A. Clarke.

NOTE

Here are some recent notable mentions around the topic of Cyber showing the national leadership of the U.S. is concerned about this domain:

- President Obama—Talked about cybersecurity in State of Union address and signed PPD-21: Critical Infrastructure Security and Resilience [1].
- Director of National Intelligence James Clapper told Congress that cyberattacks and cyberspying can damage critical infrastructure like power grids. But in prepared testimony, he says advanced cyber-actors like Russia and China are unlikely to launch such attacks unless they are threatened by conflict [2].
- Defense Secretary Leon Panetta has also been a strong advocate for increased governmental grip on the web and in October warned that the U.S. is facing a possible "cyber-Pearl Harbor" by foreign hackers [3].
- Homeland Security Secretary Janet Napolitano issued the warnings Jan 2013, claiming that inaction could result in a "cyber 9/11" attack that could knock out water, electricity and gas, causing destruction similar to that left behind by Hurricane Sandy [3].
- Representative Mike Rogers, a Michigan Republican who leads the House Intelligence Committee, has said foreign intruders "are stealing literally billions" of dollars from companies [2].
- Army General Keith Alexander, head of U.S. Cyber Command and the National Security Agency, called cybercrime "the greatest transfer of wealth in history" [2].
- Chief of Staff of the U.S. Air Force Gen. Mark Welsh III said he worried the investments made in cyber could be disappearing into a "black hole." Welsh will wait until he understands the cyber topic better, he said [4].
- Commander Army Cyber Command Lieutenant General Rhett Hernandez: Army Cyber Command/Second Army said he is tasked to operate and defend all Army networks and prepare for full-spectrum cyber-operations to support our forces worldwide [5].

We also see touches of cyber warfare in the movies starting with *War Games* in 1983 where a kid breaks into a military network and accidently almost starts World War III to *Sneakers* in 1992 where all data encryption is compromised to *Swordfish* 2001 where intelligence agencies use hacking to support their activities to the epic *Die Hard 4: Live Free* or *Die Hard* in 2007 when criminals pose as terrorists and take down the Internet and all the critical infrastructure it supports. There are a lot of great books and movies not mentioned but this sample list points to the evolution of Cyber Warfare into mainstream thinking and how it can be used as a tool to conduct espionage, crime, terror, and warfare.

America's information dominance tools, which helped win the Cold War, have become its Achilles heel of the cyber conflict we are in today. U.S. technology was far ahead of any competitor nation and we outspent them to keep the edge. Today we are more dependent on this technology than ever before, most of which is now available to our partners, competitors, and adversaries. At the same time the cost of entry into this arms race is incredibly low. Furthermore, the benefits of attacking someone far outweigh the dangers. This has led to what many are calling a Cyber War.

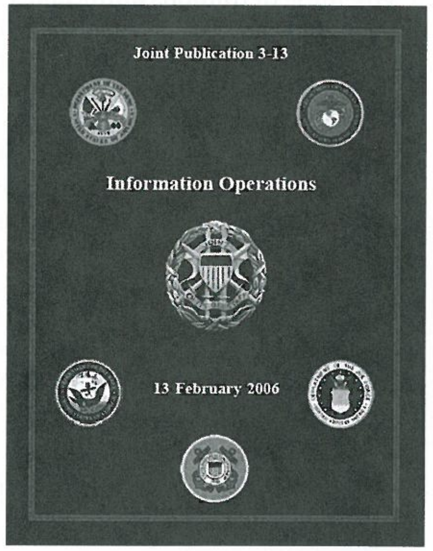
Definition for Cyber Warfare

A definition of Cyber Warfare is not easy. In fact definitions for Cyber or Warfare are both under debate. We will start with a simple definition of Cyber or Cyberspace. For the purpose of this chapter, we will frame the definition in the context of military environment.

DoD defines *cyberspace* as the "notional environment in which digitized information is communicated over computer networks" (Figure 1.1) [7]. There is no official definition for just "cyber." When you hear it by itself it could mean cybersecurity, computer network operations, electronic warfare or anything to do with the network. It is important to agree on what it means, for this book it will generally refer to cyberspace and be discussed in terms of computer network operations (attack, defend, and exploit).

The National Military Strategy for Cyberspace Operations defines *cyberspace* as the "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures" [6].

DoD (Joint Publication 3.0 Joint Operations 17 September 2006 Incorporating Change 2, 22 March 2010) defines *cyberspace* as a "global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including



Joint Publication 3-13

Information Operations

13 February 2006

FIGURE 1.1 Cyber or computer network operations falls under this doctrinal manual JP 3-13 information operations [6]. Department of Defense (DoD) joint publication 3-13 information operations 13 February 2006.

the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems. Cyberspace operations employ cyberspace capabilities primarily to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (GIG) [8].

United Nations (UN) defines cyber as "the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net." This mostly means the Internet; but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization [9].

For a definition of warfare we cannot turn to an authoritative source. The UN does not have a definition, so we will default to the two historical standards for military doctrine: *On War*, the exhaustive work documenting tactics during the Napoleonic War period in 1873 and *The Art of War* a more condensed version of how to conduct warfare composed in sixth century BC.

> ON WAR—We shall not enter into any of the abstruse definitions of war used by publicists. We shall keep to the element of the thing itself, to a duel. War is nothing but a duel on an extensive scale. If we would conceive as a unit the countless number of duels which make up a war, we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will: his first object is to throw his adversary, and thus to render him incapable of further resistance. War therefore is an act of violence to compel our opponent to fulfill our will [10].
>
> ART OF WAR—The art of war is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected. The art of war, then, is governed by five constant factors, to be taken into account in one's deliberations, when seeking to determine the conditions obtaining in the field. These are: (1) The Moral Law; (2) Heaven; (3) Earth; (4) The Commander; (5) Method and discipline [11].

Are these definitions applicable to what is happening on the Internet today? Can these historical concepts be applied to the virtual world? Is the military perspective the right one to look at this problem through? The answer to all questions is a declarative: YES. That is where this book becomes applicable: to help solidify what cyber warfare means. First there is no governing body to determine what definition we should use, so the definition is normally based on the perspective of the person speaking. Governments, finance companies, Internet providers, international corporations, organizations with a specific cause, and lawyers all give us a different answer. As for historical concepts, there are many that are based on geography which no longer apply, but most principles and practices can be modified to be useful when it comes to the new World Wide Web's Wild West. Finally, we think if we are going to use the term warfare we should use the military perspective but throughout this book we will take the time to explore the other options because our systems are connected to the same battlefield on which the nation states are fighting!

Tactical and Operational Reasons for Cyber War

The motivations for war are as old as time. Whether individuals or nations, going to war generally is based on power/patriotism/greed versus protection of self/ideology/country.

Traditionally warfare was focused on controlling limited resources but today the power of a network is not determined by resources but the number of nodes on it which equates to the power of information/influence. Additionally in some cases resources may not be as important as ability to react quickly or cycle time. Be it access to proprietary information, classified networks, interconnections on a social network, applications, or data about customers or systems that run the critical infrastructure, the more connected, the more value.

NOTE

The tactical level of war is where individual battles are executed to achieve military objectives assigned to tactical units or task forces. In the Army this would normally be at the Brigade/Regimental level.

The operational level of war is where multiple battles are combined into campaigns within a theater, or larger operational area. Activities at this level link strategy and tactics by establishing operational objectives needed to achieve the strategic objectives through a series of tactical battles. This would normally be at the Joint Task Force or Division level.

The strategic level of war is where a nation, or coalition of nations, determines national political objectives that will be enforced by military forces and other instruments of national power. This is normally controlled at the Combatant Commander level and higher.

Today's critical infrastructure networks are key targets for cyber attack because they have grown to the point where they run the command and control systems, manage the logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities. More importantly today, most command and control systems, as well as the weapon systems themselves, are connected to the GIG or have embedded computer chips. Airplanes have become flying routers receiving and sending targeting information constantly. Air Defense and Artillery are guided by computer systems and they shoot smart munitions that adjust their flight based on Global Positioning System (GPS) updates to guide themselves to the target. The Intelligence Surveillance and Reconnaissance systems gather so much information the challenge is sifting through it to find the critical data. Today's infantry squad has communication gear, GPS, tracking devices, cameras, and night vision devices. The computer chip is ubiquitous and has become one of the U.S.' centers of gravity. It is both a nations' strength and could be turned into our weakness if taken away. The loss of GPS satellites would take away many of our advantages on the battlefield.

When we consider the military maxim "amateurs study tactics; professionals study logistics," [12][a] it quickly becomes clear how important the logistical systems are. When we deploy forces into a theater of operations our capability to fight is shaped by the forces, weapons, equipment, and supplies that can be moved to the right place at the right time. Today, that is calculated and controlled by computers. An enemy can understand our intentions and abilities by tracking what is happening in the logistics system. If they can modify actions and data, they can interdict, or at least impact, our capabilities.

[a] There is much dispute as to who uttered this military maxim. It has been attributed to General Omar Bradley and U.S. Marine Corps Commandant General Robert H. Barrow. In various other forms, it has also been attributed to Napoleon, Helmuth von Moltke, and Carl von Clausewitz. For the purposes of this book, its origin is far less important than its message.

We have discussed the tactical and operational considerations now let us look at the strategic reasons to fight on the cyber front.

Cyber Strategy and Power

There are some general principles we should look at when analyzing the virtual world. When deciding on military strategies we look to the Principles of War. When evaluating plans we evaluate ends, ways, and means. When we analyze sources of national power we weigh Diplomatic, Information, Military and Economic (DIME) factors. Finally when we think of the national level tools we break them into hard power, soft power, and smart power. We will look at how all these apply to cyber warfare.

The U.S. Principles of War are Objective, Offensive, Mass, Economy of Force, Maneuver, Unity of Command, Security, Surprise, and Simplicity [12]. As we look at cyber war we must decide if we are talking about the virtual battlefield of the Internet or the ubiquitous nature of cyber conflicts being enmeshed into the physical battlefield. Some of the principles do not easily transfer into the virtual battlefield but they all can be force multipliers in the physical battlefield. When deciding on a cyber strategy we must not throw out hundreds of years' worth of doctrine and tactics but rather understand how to modify them based on the new paradigm we are facing. This has been true of all the technical advancements on the battlefield that have caused a Revolution in Military Affairs. Looking at the traditional principles of war we see having a clear *objective* with a simple plan that utilizes surprise while protecting our infrastructure is still the key to success. The numerous news stories we see show that defending in cyber warfare is not easy, so *offensive* actions are still the best way to achieve victory (this is a military statement and ignores the legal/policy challenges that must be solved). *Mass* is still important to achieve impacts and is validated by botnets today. *Unity of Command* is key for command and control. *Security, Surprise* and *Simplicity* are important for any plan, real world or virtual. *Economy of force* and *maneuver* are more difficult to apply in a battlefield with attrition and terrain being relative terms.

WARNING

Botnets are large groups of computers networked together that use their combined computing power to accomplish missions like solving complex mathematical problems or, more nefariously, to cause denial of service attacks. These groups are built from vulnerable systems with no concern for to whom they belong. Our work system, our home computer, or the MRI system at the hospital all can become zombies on a botnet if they are not protected and monitored.

When developing a strategic framework to determine how to defeat the enemy center of gravity it is important to validate the plan by analyzing ends, ways and means. "Ends" is the objective, such as deny access to enemies command and control systems. "Ways" is the form through which a strategy is implemented, such as Computer Network Attack or full scope Information Operations. "Means" consists of the resources available, such as people, equipment, and technology to execute the plan. We will look more closely at the "means" when we analyze the sources of national power. Once we develop the plan that utilizes the principles of war we use Ends/Ways/Means to validate whether we can execute it.

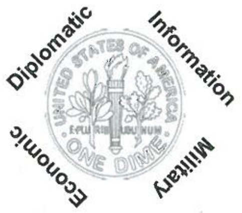


FIGURE 1.2 Instruments of national power that could influence or be influenced by cyber actions [6].

When evaluating sources of national powers we analyze the *DIME* factors seen in Figure 1.2. *Diplomatic* is based on the actions between states based on official communications. It can go through organizations like the State Department, National level Computer Emergency Readiness Teams (CERT), treaty organizations like North American Treaty Organization (NATO), economic groups like the Group of Twenty Finance Ministers and Central Bank Governors (G20), or law enforcement agencies. Next is *information.* This power is based on controlling the key resource of the information age. It encompasses strategic communication, news and popular media, international opinion, social media sites, and Open Source Intelligence (OSINT) to include the collection, analysis, and dissemination of key national actors. *Military* is the final political or government controlled option, but today we must understand this is full spectrum, from unconventional warfare, peacekeeping, humanitarian assistance, nation-building, and finally large-scale combat operations. *Economic* power comes from the influence of trade, incentives like embargos and free trade zones and direct support like aid packages or sale of surplus DoD equipment. All these factors can be applied to effect behaviors in cyber warfare.

Note that the concept of what constitutes instruments of national power is under review but the key counter insurgency doctrinal manual (FM 3-24) still uses DIME. Other acronyms are: MIDLIFE (Military, Intelligence, Diplomatic, Law Enforcement, Information, Finance, Economic), ASCOPE (Areas, Structures, Capabilities, Organizations, People, and Events), and PMESII (Political, Military, Economic, Social, Informational, Infrastructure) [13].

With cyber warfare impacting the tactical, operational, and strategic levels of war both directly and indirectly, should we move to mitigate the possibility through international agreements?

NOTE

The U.S. military has six INTs that they use to manage intelligence collection. They are Open Source Intelligence (OSINT), Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT), Technical Intelligence (TECHINT), and Measurement and Signature Intelligence (MASINT). The information from all these sources is fused into all-source analysis.

Cyber Arms Control

One idea that has become popular lately related to cyber warfare is the concept of arms control, or deterrence. The analogy is to the Cold War, where everyone understood the concept of Nuclear War being impractical because it would cause Mutually Assured Destruction (MAD). There were just a few countries that could develop nukes so they worked together to avoid a war. The thought is that if we can make cyber attacks expensive, or the consequences extremely painful, nobody would use it. This worked in the nuclear case because the cost of entry into the "Nuclear Capable" club was expensive and those in the club were all committed to not let anyone else in. Once both sides had the capability to kill the other side multiple times it led to a series of incidents that convinced both sides it was a no-win situation. Eventually a progression of international agreements reduced this threat. But MAD was an all-or-nothing scenario so is not a good fit for cyber warfare; let us look at another arms control agreement.

Another analogy are the international agreements on Biological Weapons from the 1970s. The issue is closer to cyber warfare in that it's easier to gain access to the weapons—if someone released a bio weapon it could impact the sender as much as the target, and once released it is impractical to control. The same problem exists with a computer virus released against a specific country; once someone reverse engineers it they could quickly send it back. The dangers were so intense that many countries agreed not to develop bio weapons. The challenge here was one of verification. It is impossible to track everyone who can develop these capabilities. Another challenge is there was not a dual use for bio weapons like there is for many of the malware weapons developed today. So with many groups having different goals or business plans (in the case of the criminal organizations) it is not a fair comparison.

Generally, when we talk about arms control it refers to Weapons of Mass Destruction (WMD), when we talk about cyber WMDs they are Weapons of Mass Disruption. There is no way to calculate the damage today. Rarely would a cyber attack result directly in deaths but could disrupt vital services that result in the damage to property, economic loss, or impacts to national security. This is not to say the potential is not there and we could see this become a method used by terrorists, but we are not seeing it today. The Cyber Policy Review of 2010 stated that industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion [14]. McAfee, Version and Symantec subsequently published reports ranging from trillion to 400 billion to 100 billion but there is no systematic analysis with empirical data to date. Most folks feel it is hard to justify raising cyber actions to the same level as systems that can cause mass causalities. The counter argument is there are so many critical infrastructure systems dependent on it that the unintended consequences of taking down major parts of the Internet could cause devastation at the national emergency level. As we approached year 2000 (Y2K) there was a lot of concern that systems all over the Internet would fail due to an error with how they handled calculating the date. This Y2K scare grew to the point that if we did not get everything patched we would find ourselves living at a tribal, apocalyptic level.

NOTE

There have been a lot of events like Y2K over the history of the World Wide Web (WWW) or as it is more commonly called today, the Internet. As you read this book there will be times when it would help to see them in a timeline, so we have provided a major event list by year in this book's appendix entitled, "Cyber Timeline."

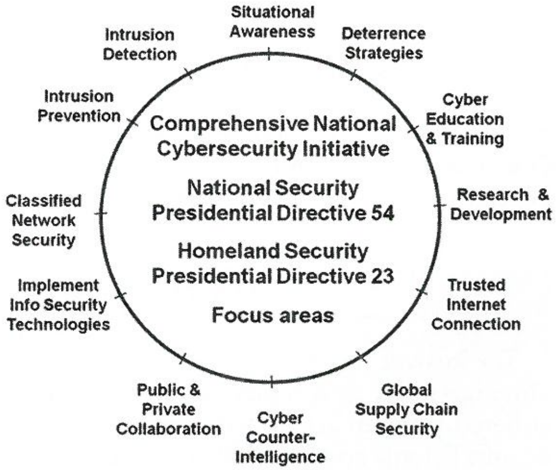
Internationally, there was an effort as early as 2005 in the United Nations to establish a cyber treaty. There was a disagreement between the United States, which had concerns about human rights violations thinking it could be used to suppress dissents, and Russia, which was pushing

for banning military actions in cyberspace. No verification process was laid out and it quickly died. Then in mid-2010 it came back with 15 nations supporting a modified version of the plan. The supporters were: America, Belarus, Brazil, Britain, China, Estonia, France, Germany, India, Israel, Italy, Qatar, Russia, South Africa, and South Korea. They compromised and focused on areas they could agree on like: establish accepted behaviors in cyberspace, exchange information on national laws and strategies, and strengthen computer protection in underdeveloped countries [15]. More recently, the EastWest Institute's Bilateral on Critical Infrastructure Protection committee published "Working Towards Rules for Governing Cyber Conflict—Rendering the Geneva and Hague Conventions in Cyberspace" which proposed joint recommendations for the private sector and governments. The European Commission has also made progress by publishing the Joint Communication to the European Parliament, the Council, The European Economic and Social Committee, and the Committee of the called "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" laying out guidelines of behaviors. Finally, the Tallinn Manual on the International Law Applicable to Cyber Warfare was a positive collaboration how current laws map to cyberspace. Cyber is an international problem so a key part of the solution is these international agreements.

What is the United States Doing about the Threat of a Cyber War?

As the Internet started to become critical to running governments and economies, it soon became both an advantage and a valuable target. For the nations that operate in the information age it is a key enabler, for the emerging nations it offers them the ability to leapfrog many competitors, for those still fundamentally in the agricultural age it offers an ability to conduct asymmetrical operations. For the United States, it is a part of all our national strategies, with numerous presidential directives to include the George Bush Sr administration's heavily funded Comprehensive National Cybersecurity Initiative [16] designed to address the National Security level concerns as seen in Figure 1.3.

FIGURE 1.3 The 12 areas where the Bush administration invested in cybersecurity.


Situational Awareness
Deterrence Strategies
Cyber Education & Training
Research & Development
Trusted Internet Connection
Global Supply Chain Security
Cyber Counter-Intelligence
Public & Private Collaboration
Implement Info Security Technologies
Classified Network Security
Intrusion Prevention
Intrusion Detection
Comprehensive National Cybersecurity Initiative
National Security Presidential Directive 54
Homeland Security Presidential Directive 23
Focus areas

NOTE

Asymmetric warfare (sometimes called Irregular Warfare or Unconventional Warfare) is war between a dominant force and a smaller force where the smaller force uses indirect or guerrilla tactics rather than to engage in force-on-force battles.

The benefits of cyber espionage/attacks are high, with so much information being available. The costs are low, with remote access being easier than physical access in many cases. The risks are lower, with few laws governing cross-border Internet activity and attribution being so difficult. Though the costs of entry are low for basic capabilities, the more industrialized countries are developing advanced espionage and attack capabilities that can impact command and control systems, weapons, and classified networks at both the software and hardware levels.

During his first term, President Obama moved to define the cybersecurity problem by commissioning the Cyberspace Policy Review [17]. Seven months after the report was released, President Obama appointed a cybersecurity policy official, "cyber czar," responsible for coordinating the nation's cybersecurity policies and activities. Then finally he authorized the DoD stand up US Cyber Command in 2010. In 2011 he signed "International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World." More recently, he has signed Presidential Directives on cybersecurity. There seems to be more emphasis on cyber in his second term but there is not much hope for any legislation around cybersecurity because of current congressional gridlock.

There are currently two major players in the protection of the nation's networks. First is the Secretary of Department of Homeland Security (DHS) which has established the U.S. CERT, published the National Incident Response Plan that included a Cyber Incident Annex and fielded the Einstein malicious cyber activity early warning system to all Federal departments and agencies (note the Einstein program is being phased out and replaced by system coming from National Security Agency (NSA) called Perfect Citizen). On the downside the DHS has suffered from a lack of a cyber budget, difficulty in hiring the right skill sets, and revolving door leadership challenges. The second major player is the dual-hatted Commander of U.S. Cyber Command (CYBERCOM) and NSA. Looking at budget, available personnel, and capabilities across the exploit, attack, and defense functions this individual will have the largest set of capabilities.

Although the United States has taken steps to address the cyber war concern, it is not ready to deal with a cyber war today. Many other nations have taken similar steps. The United Kingdom and Australia published *Cyber Strategies* in 2009 and have taken both organizational and legislative actions to secure their networks. Russia and China have taken public steps to address internal cybersecurity but have not done well with the international community as good cyber citizens. Organizations like NATO have very active cyber communities. Countries like India, France, Israel, Brazil, South Korea, and Estonia are emerging as cyber players moving to center stage.

HAVE WE SEEN A CYBER WAR?

The answer depends on the definition. To date no nation has declared a cyber war and, although many governments have spoken out about cyber activities, none have stated they suffered from an act of war. The two more talked about events are the 2007 cyber attacks against Estonia and the 2008 integrated cyber and kinetic attacks against Georgia. These both involve nation states and call on military action. There are many other incidents. Most have been called criminal acts. This trend is very reminiscent to the U.S. definition of terrorism. The United States had a low level of terrorist acts because they were all listed as criminal acts, then after the Oklahoma bombing and 9/11 they updated the definition based on new priorities and the number of incidents shot up.

NOTE

Code Word—A word or a phrase designed to represent a program or activity while remaining inconspicuous to folks not cleared for the information. A code word should be assigned randomly and have no association with the program or activity it represents. Active code words are classified. If the name is compromised it is canceled and a new name is issued.

Historically, there have been a number of high visibility cyber incidents that could qualify as cyber attacks. Here is a short list of code word programs that have been exposed:

- Eligible Receiver—This was an exercise where NSA's Red Team conducted a no-notice Vulnerability Assessment/Penetration Test of critical government networks to include the DoD. The report showed the network was so poorly protected, the results were quickly classified.
- Moonlight Maze—A series of probes and attacks starting in 1998 against the Pentagon, National Aeronautics and Space Administration, as well as affiliated academic and laboratory facilities. These attacks were tracked back to Russia but as they will not cooperate in an investigation, it could not be proven whether it was state run, local hackers, or someone routing through their systems. This is still an open investigation.
- Solar Sunrise—A series of probes and attacks in 1998 that were initially believed to be Iraq intelligence breaking into DoD systems. This was a big wake up call for the military. However, it turned out to only be a couple of kids from California who were being taught how to break into systems by an Israeli hacker.
- Titan Rain—The name given to the systematic probes and attacks against both the DoD and the Defense Industrial Base that supports it. This was originally discovered around 2003 and made its way into public media when Shawn Carpenter for Sandia National Laboratories spoke out. These activities gave birth to the name "Advanced Persistent Threat" which is commonly used today to refer to the nation state level attacks.
- Buckshot Yankee (also known as Rampart Yankee)—An attack in 2008 designed to use thumb drives as the attack vector. A variant of an older worm called agent.btz got onto both classified and unclassified networks. This resulted in the banning of thumb drives on DoD networks which had an operational impact as workarounds were needed anywhere thumb drives had been used to store, collect, or transfer information.

TIP

Many of these compromises can only be detected by things like changes to a system's performance (machine hard drive being active when no one is logged on or the system is unusually slow) or monitoring traffic exiting the network (it is easy to see a connection from the Pentagon to a system in Russia causing a concern but the attackers are getting better at hiding this). It is a good idea to check what process you are running, review your logs, and occasionally monitor outbound traffic to make sure it is all authorized.

Case Studies

Now to look at some major events that were not code word events. First we will touch on Estonia. The Estonian government had leapfrogged from a paper-based government to a web-based infrastructure to conduct all business in the 1990s. In 2007 a statue of a Soviet soldier in the capital, Tallinn, was moved from the city center to a war cemetery. As part of the outcry from the Russian population (both in Russia and those of Russian heritage still living in Estonia) this resulted in a large-scale denial of service attack against most of the day-to-day government services, news sites, banking, and e-commerce. There is a lot of speculation on whether or not this was state directed/sponsored, or just spontaneous. If the Russia government was involved, was it a low level Russian official acting on their own or directed from official channels? Regardless, when a sovereign state is prevented from conducting its functions for two weeks it is clearly a national security issue.

Estonia called to NATO for support to fight off this attack. NATO sent military personnel with technical skills needed to defend against and recover from these attacks. Estonia has gone on to become one of the leaders in the area of Cyber Strategy and today hosts the NATO Cooperative Cyber Defense Center. Was this the first cyber war? By the simple definition of a "war" as an activity between two nations, then no; but if a nation calls upon its wartime treaty for protection many would say, yes, by definition it is a war.

Next we will look at the cyber attacks during the war in Georgia, over South Ossetia. South Ossetia became de facto independent from Georgia in 1991 but remained commonly recognized by the international community as part of Georgia. A peacekeeping force of Russian and Georgian forces controlled the region. In August 2008, hostilities flared and Georgia moved forces into South Ossetia to quell separatist activities. Russia counterattacked to protect South Ossetia citizens.

Before they attacked there was a cyber recon of Georgian networks and then a series of attacks. There were web page defacements, denial of services attacks against government systems, specific malware launched and spamming email flood attacks. There were also issues with traffic getting out of Georgia (turns out it is a bad idea to have the communication pipes running through the enemy's territory). It was a well-coordinated effort run by a group out of Russia. Again there was no clear evidence of state direction or sponsorship, but information given out via the Internet regarding methods for attacking Georgia, when and what to attack, and lessons learned correlated well with the Russian offensive. So this coordinated effort was not directly attributable to the Russian government/military but did result in a cyber blockade that helped make the Russian attack more successful.

Israel has had a number of cyber warfare-related events that cross from military using cyber to patriotic citizens entering the cyber battlefield on their own. In 2007 Operation "Orchard" used cyber to impact Syria's air defense systems. In 2009 Operation "Cast Lead" Israeli websites, mostly commercial, were defaced. A pro-Palestinian attack tool was used named after a Palestinian child allegedly killed by Israeli soldiers in 2000. On the pro-Israeli side a voluntary botnet called "Help Israel Win," was deployed. These cyber conflicts continue to flare up as recently early 2013 when "#OpIsrael" started attacking Israel to be countered by the "Israeli Elite Strike Force" which attacked sites in multiple countries warning they were willing to "fight fire with fire." An infamous group of hacker called Anonymous has also gotten involved by attacking websites, Facebook pages, Twitter accounts and bank accounts in what they call "Operation Israel." In retaliation the Anonymous site was hacked and set up to play "Hatikvah," Israel's national anthem.

Next we will look at an incident that fits into a gray area around the critical aspect of national power "Economic" that could become the type of incident that leads to hostilities. In 2010, Google announced they had been attacked by elements believed to be from China. Google was one of many high-level companies that had been attacked to gain access to information on dissidents and proprietary information. This event became known as Operation Aurora and there is some interesting analysis of how the attackers got access (some of the exploits were well-known exploits), but the more interesting question is how do we classify this—a crime or an act of war? First let us look at some of the events that unfolded after the attacks. Google threatened to pull out of China and stopped censoring search results. The end result was a compromise where Google agreed to operate out of Hong Kong without censorship. Google also started to openly share information with the U.S. National Security Agency (NSA) to work through this problem which reflected the importance and made it a national security matter. U.S. Secretary of State Hillary Clinton then spoke out on the incident, and called on China to conduct an investigation on the matter. China replied to these allegations by denying involvement. So we have a key U.S. company involved with a sovereign nation that pulls in the U.S. Intelligence Community (IC) and the State Department. By today's standards this was a crime, but it led to heightened tensions between the two countries and could have easily turned into a flash point.

These examples are far from complete. Studies like "Ghost Net," "Operation Shady RAT," "Unsecured Economies: Protecting Vital Information," "Night Dragon" and "Behavioral Risk Indicators of IP Theft" talk in more detail to the economic issues. Studies like "Project Grey Goose" and "Mandiant Intelligence Center Report" talk to the nature of military operations. Analysis of specific attack tools/software like Stuxnet, Flame, Gauss, Duqu and agent.btz give great insight into targeted attacks.

So have we had a cyber war? No, there has been no country that has declared a war or who has openly stated they have come under a hostile act of war. That said, the acts we have seen today could someday be deemed acts of war. Finally when there are nations making statements through the state department, calling on war treaties and developing military doctrine, we are at a level of tension that equals the Cold War.

The Debate (is it Real?)

Some will say that the current state of affairs is just the status quo. To have the kind of growth the Internet has experienced it had to be net neutral and wide open. This resulted in many vulnerabilities being imbedded into the system. Today so much is dependent on the Internet that we want it to be safe and have declared it a national security issue. Folks who do not like the term cyber war feel there is a lot of hype spreading fear about the dangers of a coming Cyber Pearl Harbor, or for the younger generation a Cyber 9/11, that is being used so the government can spend more on cyber protection and be used to erode our privacy rights.

In 2010 a debate was held called "The Cyber War Threat Has Been Grossly Exaggerated" sponsored by Intelligence Squared U.S. Four well-known cyber experts were selected to settle the matter. Marc Rotenberg and Bruce Schneier took the position that cyber war was exaggerated and VADM (Ret) John M. (Mike) McConnell and Harvard Law Professor Jonathan Zittrain stated that we are in a cyber war. The results showed: Pre-debate vote: For, 24%; Against, 54%; Undecided, 22%; Post-debate vote: For, 23%; Against, 71%; Undecided, 6%. The majority of the undecided shifted to a belief that the threat of a cyber war is real [18].

There are three recent point papers that offer a counter point to the warfare-based discussion around cyber today. "Cyber War Will Not Take Place" by Thomas Rid 2011, "The Fog of Cyberwar Why the Threat Doesn't Live Up to the Hype" by Brandon Valeriano and Ryan Maness 2012 and "Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States" by Sean Lawson 2012.

Rid argues that cyber war has never happened, that cyber war is not taking place today and that it is unlikely that cyber war will ever occur. He states that what we actually have is subversion, espionage, and sabotage (in order of increasing difficulty and impact). He also postulates that first world countries with advanced cyber forces would be better off if they openly shared their capabilities if they want to maintain their advantage on the defense [19].

Valeriano and Maness argue that the actual damage that has been caused by cyber attacks does not justify the amount of attention or resources that are being paid to it. They feel that over reaction could have negative impacts to the freedom and innovation the Internet fosters today as governments clamp down on it. They agree there are dangers but want to use proportionally and evaluate actual damage to judge cyber attacks and not succumb to hype [20].

Lawson highlights concerns with the use of major war metaphors and Cold War analogies. He covers the power of these collective story devices and how they can be misleading when used in the wrong context. He reviews current law, cold war deterrence, counterinsurgency and bioterrorism analogies. His conclusion focus on how most metaphors and analogies are not used appropriately when talking about cyber events [21].

With two distinct camps and multiple viewpoints, it may take a cyber-based event that impacts one of the DIME elements of national power to create a catalyst that will engage the "national will" and force everyone onto the same page (think Pearl Harbor or 9/11). Today, the fact is we are facing something more like the Cold War where espionage and military spending are the bullets that will determine the outcome of the war. Unlike the Cold War the cost of entry to cyber war is much lower, the ability to determine actions and attribute players much harder, and the pace of change exponentially faster so the lessons of the last war will not serve us in this one.

WHY CYBER WARFARE IS IMPORTANT

When we look at what is at stake we can see multiple critical infrastructures. The following areas are critical to national health and to a large extent are dependent on the Internet: Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Department of Defense; 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; and Transportation System and Water as laid out in Figure 1.4. These are national

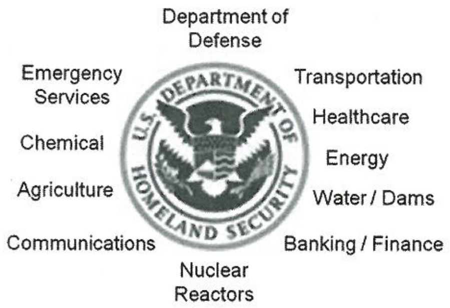


FIGURE 1.4 Critical infrastructure dependant and vulnerable to cyber attacks [22].

capabilities or programs the U.S. Department of Homeland Security's (DHS) Critical Infrastructure and Key Resources (CIKR) protection plan tracks. They work to support assessing vulnerabilities, implementing protective programs, improving security protocols, implementing real-time information sharing, and assisting with contingency planning and recovery.

Although these critical infrastructure categories were identified by the U.S. government, they are applicable to every country. Some of these are more directly involved with cyber warfare. Communications, Transportation, Department of Defense, and the Defensive Industrial Base that supports them are the most important to war fighting. Most military communications tunnel through commercial circuits so any compromise of the commercial infrastructure would effectively cut off all communications for fixed military installations.

Much of the material support the military requires is delivered over commercial infrastructure, so to lose access to rail movement, or to have supplies misrouted, could cause significant delays in operations. Finally, the DoD depends on contractors for everything from staff support to equipment development and operation.

If another nation wanted to know how to defend against the latest weapon system or wanted to clone it they would try to steal the system design documentation. The traditional method would be to try to infiltrate a spy or compromise someone working on the program. Today it would be easier to break into the servers that had the information. In the U.S., there are two locations to go after that information, the DoD program office that controls the development and fielding and the contractor that designed and builds it. So, as you can see, the infrastructure that enables most of what we do today is both our strength and our weakness.

SUMMARY

Many U.S. citizens would say the last time the *country* was at war was World War II. Others would say Korea and Vietnam were wars but technically or legally they were police actions. If Korea was a war then we are still at war with North Korea (having stood on the Demilitarized Zone (DMZ) between the two countries, many soldiers would agree). Many presidents have openly talked about the Cold War but a "war" was never declared. The United States declared a "War on Drugs" and "War on Terrorism" but those were not wars against another country but rather on problems that had reached the level that they became a national security issue.

If this is the standard we measure by then we could have a pure cyber war. We have been in multiple wars in the Middle East (Iraq twice and Afghanistan) but these were not formally declared "wars"; some would say they are part of the "War on Terrorism." The last time the United States was in a congressionally declared war was World War II; however, the concept of what a war means is changing. These have been very traditional wars and if they are the standards we measure a "war" by, then there is no such thing as cyber war.

The term "war" has taken on many different meanings over time. If we had a Cold War and are in both a Drug War and a War on Terrorism then we are in a Cyber War. If we hold to the strict nation state declaring war on another sovereign nation then we are just facing a steady state complex problem that could become an international disaster, changing economies, enabling a massive crime wave, facilitating unprecedented espionage, and creating a new domain for warfare.

Today the Internet is more similar to how the Wild West is portrayed in movies than the Cold War. Over the course of a movie, settlers might have to deal with Indian attacks, Mexican banditos, bad weather, criminals from our own community, and Mexican Army invasions. To carry the analogy to the internet/cyber domain, Indian attacks are a form of guerilla warfare, banditos are non-state actors but may have informal support from their host nation, weather equates to the environmental impacts that create noise in systems, making things unpredictable, criminal acts if they get bad enough may become a threat to the community and may require the aid of the state or federal government, and military invasion is a full-scope war that could require the full weight of the country to address. Any of these can wipe the "settlers" out and may need to be addressed by the local "sheriff," the "rangers" or the "U.S. Army" depending on the scope of the problem, demands of the people and how the government reacts. So the question of if we are in a cyber war today is answered by the simple statement: "Stop debating on what to call the problem and get us some help!"

References

[1] Whitehouse website, http://www.whitehouse.gov/cybersecurity [accessed 17.03.13].

[2] The Hill (blog), http://thehill.com/ [accessed 17.03.13].

[3] RT website, http://rt.com/usa/napolitano-us-cyber-attack-761/ [accessed 17.03.13].

[4] FP National Security website, http://killerapps.foreignpolicy.com/posts/2012/09/18/air_force_chief_wary_of_cyber_black_hole [accessed 17.03.13].

[5] Secretary of Defense. DoD Publications, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf [accessed 17.03.13].

[6] Secretary of Defense. DoD Publications, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf [accessed 17.03.13].

[7] Joint Electronic. Electronic Library Library, http://www.dtic.mil/doctrine/dod_dictionary/index.html; 2010 [accessed 17.03.13].

[8] United Nations. UN terms, http://unterm.un.org/dgaacs/unterm.nsf/375b4cb457d6e2cc85256b260070ed33/$searchForm?SearchView [accessed 17.03.13].

[9] Bassford C. The clausewitz homepage. On war [document on the Internet], http://www.clausewitz.com/readings/OnWar1873/; 2010 [accessed 17.03.13].

[10] Tzu S. On the art of war, http://www.chinapage.com/sunzi-e.html [accessed 17.03.13].

[11] Wright DP, Reese, CTR. ON POINT II: Transition to the New Campaign. The United States Army in Operation IRAQI FREEDOM May 2003-January 2005 Part IV Sustaining the Campaign Chapter 12 Logistics and Combat Service Support Operations, http://www.globalsecurity.org/military/library/report/2008/onpoint/chap12.htm [accessed 17.03.13].

[12] Joint Doctrine Division, J-7, Joint Staff. DOD dictionary of military and associated terms [document on the Internet], http://www.dtic.mil/doctrine/dod_dictionary/index.html; 2010 [accessed 17.03.13].

[13] Kem CJD (Retired). Understanding the operational environment: the expansion of DIME, http://www.thefreelibrary.com/Understanding+the+operational+environment%3A+the+expansion+of+DIME.-a0213693824 [accessed 17.03.13].

[14] Securing Our Digital Future. The white house blog, Washington, DC, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; 2010 [accessed 17.03.13].

[15] Homeland Security Newswire. 15 nations agree to start working together on cyber arms control. Business of homeland security, http://www.homelandsecuritynewswire.com/first-15-nations-agree-start-working-together-cyber-arms-control [accessed 17.03.13].

[16] The National Security Council (NSC). National security council. The comprehensive national cybersecurity initiative [document on the Internet], Washington, DC, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative [accessed 17.03.13].

[17] Securing Our Digital Future. The white house blog [document on the Internet], Washington, DC, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [accessed 17.03.13].

[18] IQ2US. Intelligence squared U.S. Debate—The cyber war threat has been grossly exaggerated, Washington DC, USA: s.n., http://intelligencesquaredus.org/index.php/past-debates/cyber-war-threat-has-been-grossly-exaggerated/ [accessed 17.03.13].

[19] Rid T. Cyber war will not take place. J Strat Stud 2012;35(1):5–32.

[20] Valeriano B, Maness R. The fog of cyberwar why the threat doesn't live up to the hype. J Strat Stud 2013;35(1):5–32. National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection no: 10 Helsinki. http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar.

[21] Lawson S. Putting the "war" in cyberwar: metaphor, analogy, and cybersecurity discourse in the United States. First Monday 2012;17(7).

[22] Department of Homeland Security. Homeland security, www.dhs.gov [accessed 17.03.13].

CHAPTER

2

Cyber Threatscape

INFORMATION IN THIS CHAPTER

- How did We Get Here?
- Attack Methodology With the Tools and Techniques Used to Execute Them
- Attackers (Major Categories of Threats)
- Defense in Depth—How Organizations Defend Today (Defensive Mountain Range)
- What the Threat is After (What We Should Focus on Defending)

HOW DID WE GET HERE?

In the early 1980s, when ARPANET was becoming the World Wide Web which grew into today's Internet, the focus was on interoperability and reliability as a means of communication and potential command and control in the event of an emergency. Everyone with access to the system knew each other and security was not a consideration. Then, in the late 1980s, trouble started; Robert Morris released the first worm (a self-replicating piece of malware) and Clifford Stoll discovered Soviet Bloc spies stealing U.S. secrets via a mainframe at the University of California, Berkeley. These were quickly followed by a number of incidents that highlighted the security risks associated with our new communication capability (see Appendix for list of major events through the years).

The key cyber events as they relate to and impacted the military occurred in the mid-to-late 1990s highlighted by Time magazine having a cover on "Cyber War." The 1998 Solar Sunrise incident hit the news as the Pentagon got hacked while America was at war with Iraq, but the instigators were actually just two kids from California. Then came Moonlight Maze, where the Department of Defense (DoD) found intrusions from systems in the Soviet Union (though the source of the attacks was never proven) and Russia denied any involvement (hackers will often route their attacks through countries that will not cooperate with an investigation so there was plausible deniability). By the early 2000s, a series of attacks, generally accepted as being from China, were identified and code named Titan Rain, the name was changed to Byzantine Hades after the Titan Rain code name was disclosed in the media and changed again when the Byzantine Hades code name was posted to WikiLeaks (current name is classified). The term "Advance Persistent Threat (APT)" has become the common reference term for this state-sponsored systematic electronic reconnaissance/digital espionage. By late 2000s, there was a physical aspect added to the entropic attacks which the DoD code named Operation Buckshot Yankee. Thumb drives used by U.S. Military were found to have malcode embedded which caused DoD to ban thumb drive usage on all military networks and systems.

In addition to attacks on the U.S. Military, some international incidents occurred in the 2000s. In 2007, hackers believed to be linked to the Russian government brought down the Web sites of Estonia's parliament, banks, ministries, newspapers, and broadcasters. Estonia called on the NATO treaty for protection and troops to help recover. A year later cyber attackers hijacked government and commercial Web sites in Georgia during a military conflict with Russia, creating a new form of digital signal jamming over the Web. In 2010, the Stuxnet worm attacked the systems that control Iran's nuclear material development causing damage to these systems. While the examples we have looked at, a nation calling on a mutual defense treaty—combined kinetic/non-kinetic war and physical destruction of a national security asset, could be considered to be cyber wars no nation state has formally acknowledged or accused another state of "cyber war."

There are some notable commercial cyber events that parallel the military's pains. In 2009, reports revealed that hackers downloaded data from the DoD's multibillion-dollar F-35 Joint Strike Fighter program, showing that the cyber attackers were going after defense contractors as well as the military itself. Then in 2009, Operation Aurora broke into the news when Google publicly revealed itself as being one of many commercial companies hacked by the APT, showing that the cyber attackers were also going after commercial intellectual property. There were two more troubling attacks in 2011: The first was a series of hacks exposed in the global energy report "Night Dragon" which showed how China was trying to gain a competitive edge in the energy market through espionage. The second was the RSA attack where stolen information would allow a hacker to replicate the number that showed up on the password token many organizations used to secure their networks, showing that the enemy was willing to attack the infrastructure used to protect the U.S. More recently, a very detailed report on China's cyber operations was published by the commercial consulting vendor Mandiant. These all point to an active campaign to steal intellectual property. Some of the information is taken to gain military advantage but the majority is to gain an economic advantage which as we look at countries' ability to fund their militaries has a direct impact.

For the past 30 years, there has been a continuous battle between defenders and attackers on networks around the globe. At first most of the hackers were motivated by curiosity, looking for entertainment or bragging rights. Then as more financial transactions were conducted on the internet, a criminal element followed. Soon we saw trends like botnets where it did not matter to the attacker if the target was military, government, or commercial, the attacker was just after as many computer systems as they could acquire. This was back in the days when it was popular to say "network security needs to be good enough so that you're not the low hanging fruit on the internet." That is no longer true as with many sophisticated threat organizations there are a lot of giraffes on the internet interested in only eating fruit from the top of the tree; security today needs to be good—not better than the next guy. Then as nation's governments, militaries and economies became more dependent on the internet

we see nation states acting against each other in cyberspace. As each new threat grows new protective solutions are established and new attacks are developed to circumvent them, and the cycle continues.

The threatscape map in Figure 2.1 was designed to assist everyone in understanding this complex environment. As we look at it some will see the map of Mordor from J.R. Tolkien's fictional Middle-Earth while others see the old TV show's map of the Ponderosa. The map is designed to show how all the events we have covered in this chapter interrelate in cyberspace. It shows the methodology (upper left) and resources (lower left) that hackers use to break into systems. Then it provides the different categories of the attackers in the second column. These categories are divided by a solid line but it is important to realize that nation states can use criminal organization to accomplish their aims or for another example where they can cross is between insider threat and hacktivists. In the past an insider might post an organizations' critical information on the internet, either because they were disgruntled or a whistle-blower, but now hacktivists are behaving like an insider threat by not stealing information but rather by posting it openly on the internet. The center column shows the defensive mountain range to portray the "defense in depth" strategy used to protect networks today. Finally, the far right column shows the different types of data the attacker wants access to. It is broken out by the motivations of the threat actors from the second column.

ATTACK METHODOLOGY WITH THE TOOLS AND TECHNIQUES USED TO EXECUTE THEM

As we examine the manner in which networks are broken into, it is evident that the basic steps in the process are analogous to traditional military attack/defend doctrine. Similar to how South Korea and North Korea have built physical defensive fortifications between each other, we see the same principle and even term used by network administrators—Demilitarized Zone (DMZ). This is where one puts systems that must connect to the internet where they are in more danger. From the attacker point of view the same steps are necessary to attack a network as it is to break through the DMZ: conduct reconnaissance to determine vulnerability, marshal forces at the point of weakness, attack and penetrate the defense, then exploit the infiltration to gain control over the battlefield/network.

The major difference between kinetic (real world) and non-kinetic (virtual world) warfare methodology is the weapons versus software programs they use. We will walk through the steps and define a few of the tools used. The tools will be covered in more detail in later chapters so this will just be to gain an initial understanding.

WARNING

The only difference between a hacker tool and a cybersecurity professional tool is "written permission." Please do not load a tool you read about here like the password cracker on an operational computer at work to test your organization's security without authorization. People have been fired for using these tools despite their good intentions. Contact your manager and get approval, in writing, then test your security in a coordinated and safe manner.

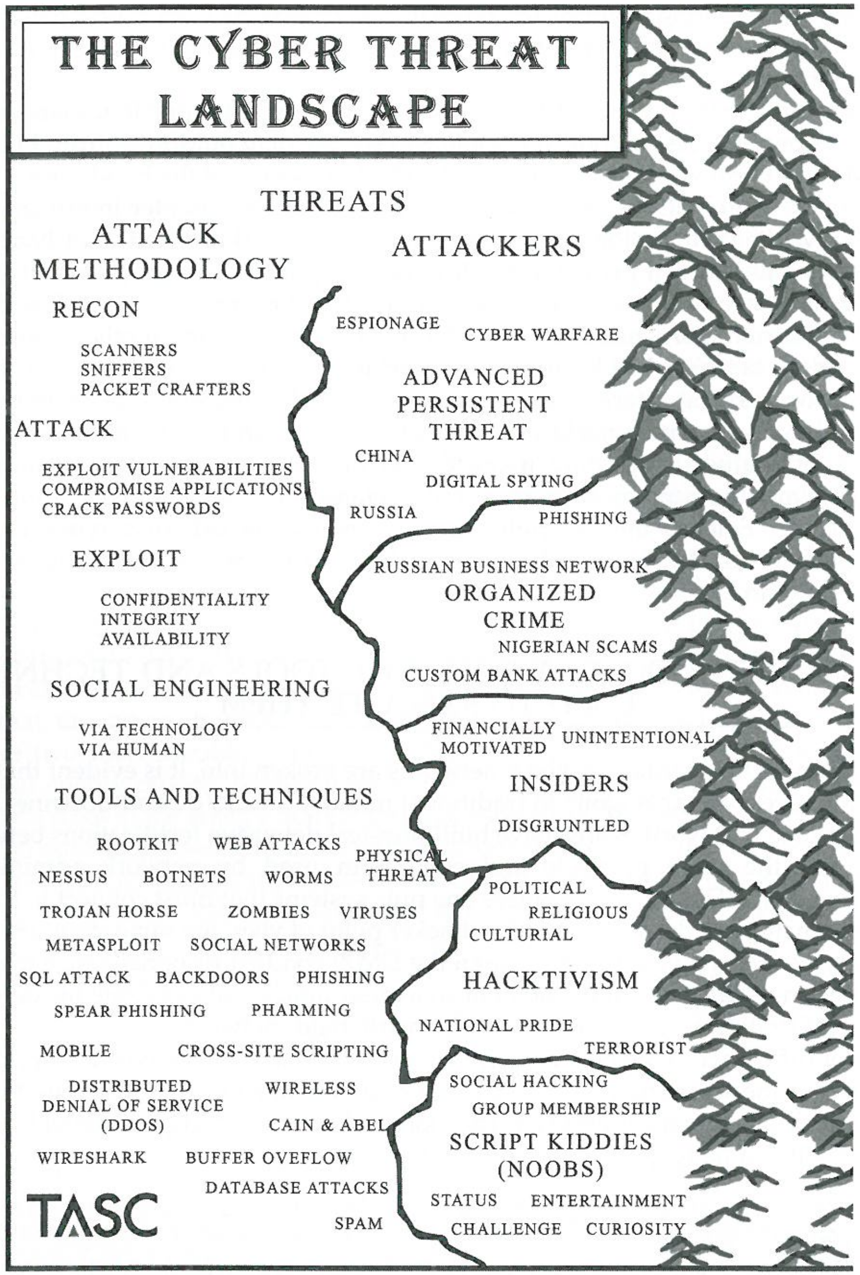


FIGURE 2.1 This is a threatscape map designed to show the different components in the cyber environment and how they interact.

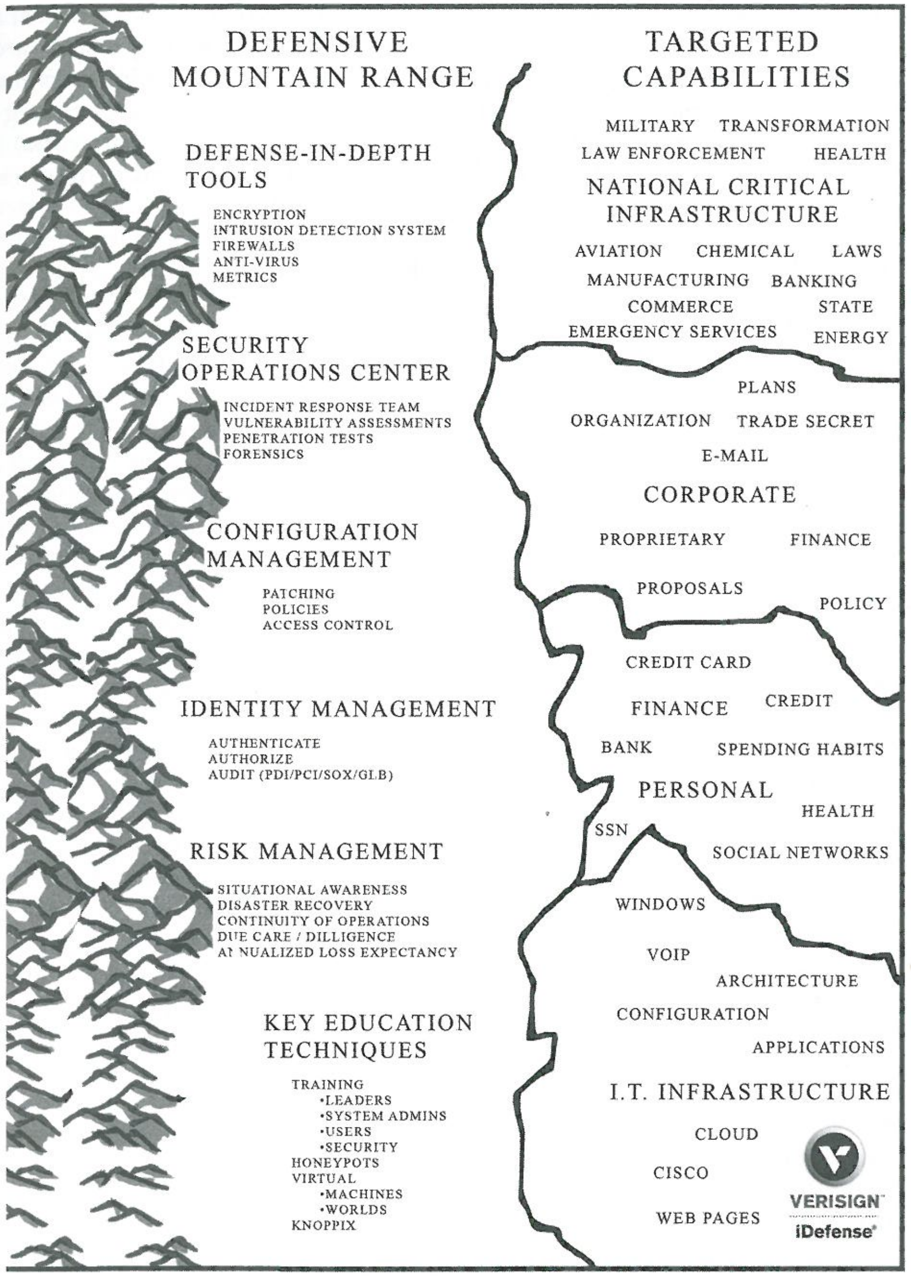


FIGURE 2.1—Cont'd

An attack methodology is the process or general steps used to conduct an attack of a target. The tools/techniques are what are used to execute the process. The major steps are recon, attack, and exploit. These steps can be a variety of activities, from launching machine to machine attacks to using social engineering. (Think of social engineering as scamming or conning a target out of information allowing the hacker to compromise a network.) Each of these steps or phases have a number of substeps to accomplish them and in many cases different hackers will both modify and automate them to suit their style.

Mapping Sample of Well-known Tools to the Process

- Reconnaissance
  - Scanners
    - Nmap
    - Nessus
  - Sniffers
    - Wiresharek
    - Ettercap
  - Packet Crafters
    - Netcat
    - Hping
- Attack
  - Exploit Vulnerabilities
    - Metasploit
    - Canvas
    - CoreImpact
    - Back Track
  - Compromise Applications
    - Web page—Cross-site Scripting
    - Database—SQL attack
  - Crack Passwords
    - Cain and Able
    - John the Ripper
- Exploit
  - Confidentiality
    - Steal data to use or expose
  - Integrity
    - Change data based on impact desired
  - Availability
    - DDOS based on critical timing
- SE
  - Via Technology
    - Social Engineering Toolkit
    - Maltego
  - Via Human or user
    - Phishing
    - Social Networking sites

To begin the recon phase a target is required. The target can be the specific systems that will be attacked or the personnel that use them. To attack the unique Internet Protocol (IP) address for a machine or Uniform Resource Locator for a Web page must be known. To conduct an attack via the users, a phone number could be all that is needed. IP addresses and phone numbers can be found with a quick Google search or with services like American Registry for Internet Numbers searches. Much of what is needed for a social engineering attack can be found on a business card.

Once the target is identified, the recon begins to find the weak point or vulnerability. The attack can be against the operating system or one of the applications on it (i.e., Adobe Flash, Microsoft Office, games, Web browsers, or an instant messenger). A scanner is run against the system to determine and list many of the vulnerabilities. Some of the more popular scanners are Nmap, Nessus, eEye Retina, and Saintscanner. Attack framework tools are available that both scan and then have the exploits to launch the attack matching vulnerabilities found built into the application. Some popular framework tools are Metasploit, Canvas, and Core Impact. Finally, there are tools that transform a machine into a Linux system by booting off of a Linux live CD. The most popular live CD attack tool is BackTrack.

Another tool that is useful during recon is a sniffer. This is a tool that has the attacker's system mimic every computer on the network so it gets a copy of all the traffic. It will allow the attacker to read all unencrypted emails and documents as well as see the Web pages being accessed by everyone on the network. Popular sniffers are Wireshark, Ettercap, and Tcpdump. On the wireless side tools include Aircrack-ng and Kismet.

While there are a lot of recon tools that are very powerful and easy to use, the one set of tools that shows how the threat environment has evolved is packet crafters. Someone with no programming skills can now craft unique attacks. Popular tools include NetCat and Hping. There are a host of other tools for recon but these represent the baseline tools used to discover the vulnerabilities that allow movement to the attack phase.

When attacking a system there are many types of malcode that can be used. At the code level there are worms or viruses that can use attack vectors like cross-site scripting or buffer overflows to install rootkits or a Trojan horse which acts as a backdoor into a system, and is used to spread the attack. A worm spreads without any help. It infects a system and then uses that system to find more systems to spread to. A virus needs some user interaction like opening any type of file (email, document, presentation) or starting a program (game, video, new app). Worms and viruses use techniques like cross-site scripting or buffer overflows which attack mistakes in the code in order to compromise it. Cross-site scripting is a Web-based attack that allows unauthorized code to be executed on the viewer's computer that could result in information being stolen or the system's identification certificates being stolen. An overly simplified example of a buffer overflow is when a program asks for a phone number rather than giving the 10 digits needed, the software sends 1000 digits followed by a command to install the malcode. Because the program does not have good error handling to deal with the large amount of unexpected extra data, it executes the malcode.

A rootkit is a program that takes over control of an operating system and tells lies about what is happening on the system. Once a rootkit is installed, it can hide the hacker's folders (i.e., hacker tools, illegal movies, stolen credit card numbers), misdirect applications (i.e., show the antivirus updating daily but do not allow it to update), or misrepresent the system status (i.e., leave port 666 open so the hacker can remotely access the system but show it as closed).

The first generation of rootkits was much like my daughter when she was 4 (called the fibbing 4s because that is when most kids learn to lie). Like a 4-year-old, the rootkits of the first generation did not lie very well. The generation we are on now is more like when she was 21 (she was MUCH better at telling a coherent story that was not easy to detect as a lie). The current generation of rootkits does a much better job of hiding themselves from detection. The next generation will be like someone with a masters in social engineering; almost undetectable. A Trojan horse backdoor is a program that masquerades as a legitimate file (often a system file: i.e., files ending in .sys on a Windows box or the system library on a Mac). These files are actually fakes and have replaced the actual system file. The new file both runs the system and opens a backdoor to the system allowing the hacker remote control of the system.

One use for worms and viruses is to build botnet armies. A bot (also called a zombie) is a computer that is a slave to a controller. Once someone builds an army of millions of bots they can cause a distributed denial of service (DDoS) by having all of the bots try to connect to the same site or system simultaneously. This can be done to blackmail a Website (pay or be blocked so no customers can get access), disrupt command and control systems, click fraud (if Acme.org gets paid one cent for every customer that clicks on link taking them to Selling.com a botnet could be used to do that millions of times a day) or compile complex problems (much like a distributed supercomputer).

NOTE

If the intent of an attack is to cause a Denial of Service (DoS) there are two ways to accomplish this. The first is to attack the system and take it down. The second (usually called Distributed DoS or DDoS) attacks the bandwidth. In cases where you are attacking the communication lines you can skip recon because you are not worried about finding a specific vulnerability, you just need a botnet army large enough to overwhelm a target's communication capabilities. If you are attacking an organization with distributed and redundant infrastructure then it would be necessary to develop malcode that attacks the organization's systems simultaneously to take it offline as it is impractical to take down all the communication capabilities.

There are a number of ways to launch attacks targeted at a specific system rather than the broad net a worm or virus would catch. The attack framework tools mentioned earlier are the most common. The key is to correlate the exploit to the vulnerability. Much like there has never been a bank built that cannot be robbed and there is not a computer or network that cannot be broken into given enough resources and persistence. If no vulnerability can be found then the attacker can go after the authentication via password attacks, credential compromises or attack the security infrastructure used to protect the network.

Cracking passwords can be done with brute force by having a program try every possible password iteration. This can be time consuming and is easy to detect but, depending on the strength of the password, is very effective. If the hacker can get access to the password file then tools like Cain & Able or Jack the Ripper can be utilized to crack them. Another technique that is available is called rainbow tables. These are databases where popular password encryption protocols have been run on every possible key combination on a standard keyboard. This precompiled list allows a simple lookup when the hacker gets access to the list of encrypted passwords. Many of these tables have done every combination for 8-20 characters and the length grows as hackers continue to use botnet to build the tables.

NOTE

Exploit has three meanings within the cyber community. When talking about code it refers to malcode that allows a system to be compromised. When talking about attack methodology it refers to what the payload of the attack is intended to accomplish. When talking about military doctrine it is used by the intelligence community to refer to cyber recon/espionage.

The exploit phase is where the attacker takes advantage of gaining control. There are generally three factors that the hacker can compromise: Confidentiality, Integrity, or Availability. When attacking confidentiality they are simply stealing secrets. Integrity attacks are when they change the data on the system or masquerade as a legitimate authorized or authenticated user. In a commercial setting this could be changing prices or customer data. On a military network it might be to change the equations used to calculate command and control guidance. Availability attacks are normally time based and can be accomplished by taking the system down or overwhelming the bandwidth. The type of exploit is based on the motivations of the attacker. They can use the system to attack more systems on the network, misrepresent the user (send fake emails), or load a rootkit with a backdoor to maintain long-term access. They will often try to avoid detection and might even use anti-forensic techniques like log wiping and time stomping. Some will patch the systems they have taken over so future hackers will not be able to break in and take them away. Finally, they may load digital tripwire alarms to tell them if they have been detected by security engineers using forensic tools.

If these technical attacks do not work another vector of attack is social engineering. In fact some threat organizations use social engineering as their primary means of attack. Social Engineering (SE) can be thought of as the act of influencing someone's behavior through manipulating their emotions, or gaining and betraying their trust to gain access to their system. The difference between social engineering and other attacks is the vectors are through the person, or as hackers say the "wetware." Think of any of the movies about stories or movies about con-artists, the difference being rather than money they want access to information on or about a target's computer systems. This can be done in person but is often done over the phone or remote communications like email. It starts with pre-texting, with includes researching an organization using sources like websites, social media, or even meeting people at places like a conference to exchange business cards. The most common attack today is via email. This kind of social engineering attack is called phishing (sending general email to multiple people), spear phishing (targeted at a specific person), or whaling (targeting a specific senior member of the organization). There are also technical tools like the "Social Engineer Toolkit" that are designed to assist attacking the workforce.

ATTACKERS (MAJOR CATEGORIES OF THREATS)

This section will focus on the different categories of attackers. As we look at the threatscape map (Figure 2.1) the attackers are not ranked or ordered in any particular way. Again it is important to note that while there are solid lines between them they can overlap or someone can belong to more than one category. The Advanced Persistent Threat (APT) can buy exploits from criminal elements, noobs can join hacktivist causes and, one particularly troubling paradigm shift that has happened recently, hacktivists can behave like insider threats as they steal information and then publish the stolen information on the websites like WikiLeaks.

Advanced Persistent Threat

APT is one of the key drivers of cyber warfare. The term APT is often used in different ways by the media, but, for purposes of this book, APT means state guided attacks. It is truly digital spying or espionage in the virtual world. Some of the most commonly referenced APT activities were discussed earlier (Titan Rain, Operation Buckshot Yankee, Aurora, Stuxnet, Night Dragon, APT1 Report). As we examine if the APT actions qualify as war we look to how war is defined.

Organized Crime

Organized crime on the Internet is widely covered in the news today. One of the most often joked about scams on the Internet is the "Nigerian royalty that just needs access to your bank account to get money out of the country" scam that sends phishing emails designed to steal identities and access the victims' bank accounts. The text of the emails from the Nigerian scams will talk about how they have money that they need to get out of the country and all they need is to transfer the money to a U.S. bank, but to do that they need access to the victim's account. The early versions used poor English but they have gotten much more sophisticated over time. These scams have been around long before the Internet but have become much easier to do in bulk and with little risk of incarceration, as the perpetrators are usually overseas. Another popular scam is selling fake medicine. While some of the sites are selling legitimate drugs most will send fake medicine if they send anything at all. Similar scams can be used to get members of the military or national security infrastructure to get involved in activities they would not do in the real world.

One of the more well-known criminal organizations is called the Russian Business Network (RBN) also known as the Russian Mob (note this is not one single organization). If someone graduates from a university in one of the old Soviet Union bloc countries with a degree in computer science one of the better paying jobs is with the RBN. There they will work full time on tasks like building custom exploits targeting specific financial institutions, building botnet armies, running identity theft networks, or any one of a dozen of "business ventures" for organizations like the RBN based on different revenue models. These organizations can be staffed in one country, use systems hosted in a different country (for a while RBN was using systems hosted in China) and commit crimes against citizens in a third country. This makes it very complex to prosecute when the crimes are discovered. A great reference that goes into detail is the book "Fatal System Error" by Joseph Menn. While we have talked about China and Russia they are not the only countries that have cyber-based criminal organizations; in fact the U.S. has similar groups.

Insider Threat

As we change to look at insider threat you will find a common rule of thumb is that insider threats represent 20% of the threat but could cause 80% of the damage (recent studies by CIS and Verizon show the real numbers of insiders are closer to 50%). The reason is the insiders understand what is valuable on the network and often have legitimate access to it. The three basic categories of insiders are: disgruntled employees, financially motivated (thieves), and users unintentionally causing damage. Disgruntled employees can cause problems by publishing information on the Web to competitors or to fellow employees (i.e., everyone's salary). They could also install a logic bomb that will cause damage if they stop working at the company (i.e., if Winterfeld does not show up on the employee payroll, reformat all servers in the data room). Financially motivated insiders will misuse the company assets or manipulate the system to steal. There are both intentional and unintentional insider threats. Examples of unwitting threats include users who unintentionally delete files causing loss of work or accidentally post classified documents on unclassified systems causing what is known as a spill. Spills could require destruction of the system and a lengthy investigation. Finally, users can open files or go to websites with malcode infecting the network.

Hacktivist

Hacktivists can be motivated by political views, cultural/religious beliefs, national pride, or terrorist ideology. The most notable example has been from a group called Anonymous. This group of loosely affiliated hackers from around the world banded together to attack organizations they felt were in the wrong. This cyber vigilante group attacked the Church of Scientology under project name Chanology in 2008 and started using their trademark saying "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us" [1]. They have attacked MasterCard for stopping support of WikiLeaks, Law Enforcement Agencies for policy they do not support, political parties, HBGary Federal (in response to statement made by Aaron Barr), Sony (in response to a lawsuit they brought), the Bay Area Rapid Transit system (in response to their closing down cell phone tower coverage at the stations to prevent a protest), porn sites, and many government sites around the world. Their supporters can often be seen wearing Guy Fawkes masks from the movie "V for Vendetta." As of early 2013, the FBI has arrested many of the leaders of Anonymous, but the group is still active and expect more groups like this to sprout up. A good reference to read on the story is "We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency" by Parmy Olson.

Script Kiddies/Noobs

The final group in this section is on Script kiddies or noobs (for new to hacker). These are pejorative terms for the less skilled hackers. These are the people who just use the tools that can be found on the Internet with little thought out methodology or technique. They have many different motivations to start hacking. Some are looking for a social experience and will try to join a hacker group (some groups will require proof of hacking ability before they grant membership), others enjoy the challenge or want to gain status across the hacker community, still others do it out of curiosity and think of it as entertainment. We can see many examples of these at hacker conferences like DEFCON, ShmooCon, or HOPE. The problem these script kiddies pose to the cyber warfare landscape is the amount of activity they produce. If there are millions of attacks launched by noobs every week, how can the APT or specific criminal activity be located? It is also important to understand that the tools script-kiddies use are very powerful and they will end up PWNing (slang for own) systems. The age old adage "the defender has to get it right every time while the attacker only has to get it right once" applies here. The Defense Information Systems Agency has consistently said the majority of systems compromised were from known exploits that could have been prevented if the systems were fully patched and configured to standard [2]. As script-kiddies gain more experience they will become hackers and usually end up being part of some group.

These groups are not represented in the threat list as they do not fit into an attacker category. When they join together they may prank each other, build tools (one classic example is the Cult of the Dead Cow's tool called "Back Orifice" in 1980), they may live near each other (i.e., 303 group in Denver), skill focused (Social-http://www.social-engineer.org/ group), startup conferences (B-Sides) or run a podcast (pauldotcom). This would be an example of the range of motivations—some are white hat and only use their skills when professionally contracted to test security, others are gray hat and do what they feel is the right thing for betterment of the Cybersecurity community and some are black hats who conduct illegal activities.

DEFENSE IN DEPTH—HOW ORGANIZATIONS DEFEND TODAY (DEFENSIVE MOUNTAIN RANGE)

On the threatscape map (center column of Figure 2.1) the Defensive Mountain Range shows many of the different methods used to protect networks today. It covers the infrastructure and processes used to secure the systems and detect any intrusions. Much like real-world defenses, they need to be constantly validated, monitored, and updated.

Defense-In-Depth or multiple layers of protection is how most networks are protected today. The issue is there are so many mobile systems (laptops, phones, tablets) and removable storage devices that it is becoming increasing difficult to keep all the systems inside the defensive perimeter. Some of the critical tools are firewalls to block the attacks, intrusion detection systems to alert on attacks, antivirus to kill the attacks that got through, and encryption of the data on the device so if the device is lost or stolen the information is still secure. The critical process needed is good security metrics. Metrics revolve around the need to quantify the impact of cyber events. They should support both the technical and senior leadership's ability to make decisions to protect the network and react to changes in risk assessment as well as support understanding of return on investment of security infrastructure. There has been a lot of work done, but there is no clear set of industry standard cyber metrics today. There are three basic types of metrics:

- *Technical:* Based on infrastructure and the incident response cycle.
- *Security return on investment:* Cost-based analysis on benefits from implementing new technology or policies. These goals must be set before they change and methods to track performance are established.
- *Risk posture:* Analysis on impact of cyber events/incidents to enterprise and operations.

Next comes the team that monitors the network, usually called the Security Operations Centers (SOC) or Computer Emergency Response Team. These cells typically contain the Incident Response Teams responsible for the response cycle—Protect, Detect, React, and Recover. This is very similar to the military OODA Loop (Observe, Orient, Decide, and Act). The SOC would also be responsible for conducting Vulnerability Assessments (VA) and Penetration Tests (PT). The VA is designed to look for vulnerabilities on the network then prioritize how to fix or mitigate them. The PT is designed to test the team's ability to respond to an intrusion. Penetration Tests can also be called Red Teaming depending on the scope and interaction of the two sides. The PT team will not only find the vulnerability but exploit it and once they break in will either grab a predetermined file (called the flag) or load a file on the system (called the golden nugget). Then the SOC team must determine how the PT broke in and what they did. This will validate the team's processes and tools. One key capability that is needed after an intrusion is the forensics expert. This is someone that understands the rules of evidence and can testify in court. This analysis is key to understand what happened to prevent it from reoccurring.

TIP

A forensics expert is a must-have team member, but, as they can be expensive, many organizations have someone they can call on demand as opposed to having a full time staff member. The forensics expert should be called if there is any possibility of a lawsuit, human resource action (firing), or prosecution of the hacker. There must be clear policies on when they are called because, much like a real crime scene, the more people that have accessed the data the more the crime scene is compromised. The military is slowly moving toward gathering evidence in a way that it can be presented in court as opposed to just getting the systems back on line quickly.

Configuration Management is a critical part of the defense. A well-configured and managed network is more secure. Think of walking up to a cruise liner to start your vacation only to find it is so covered in rust you cannot tell what color it used to be painted. Common sense would prevent you from getting on. Yet because we cannot see that our network devices are past their maintenance lifecycle we put our most valuable information on the equivalent servers. The basics require timely patching. Patches must be tested before they get installed on critical operational systems so the challenge is how much time is allowed for analysis (some suggest 72 h, but that can be expensive so there is a broad range). Well understood and enforced policies for both the users and network administrators are a must. They both can impact the security baseline with decisions on operations or processes but often do not examine the impact to security risks. Finally, access control must be managed so that only the people with a need are allowed to access the mission critical data. This can be done physically or through electronic policies. This is called the principle of least privilege and has been used for decades in the intelligence community.

Identity Management is one area that will help as users become more mobile. The three vital factors are authentication, authorization, and audit/compliance. Before someone logs into the system they should have to prove who they are with something they know (user name and password), something they have (electronic token), and/or something they are (biometrics, i.e., scan a fingerprint): this is authentication. Next they should be categorized by what kind of information they should have access to. The military uses Unclassified/Secret/Top Secret but there are a number of organizations that have designed their own system. Finally, as was mentioned earlier, as every network will have a weakness over time it is prudent to assume that someone has penetrated the network and conduct audits to find them.

Compliance is based on the legal or regulatory requirements of the industry. Some examples are:

- Healthcare = Health Insurance Portability and Accountability Act (HIPAA)
- Finance = Gramm-Leach-Bliley Act
- Publicly traded companies = Sarbanes-Oxley Act
- Credit Cards = Payment Card Industry
- Energy Providers = North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program
- Federal agencies = Federal Information Security Management Act (FISMA)
- U.S. Intelligence Community (IC) = Director of Central Intelligence Directive (DCID) 6/3
- DoD = DoD Information Assurance Certification and Accreditation Process (DIACAP)

Today most of these are based on annual reviews of the systems but they are moving to real-time monitoring.

Risk Management is what all these regulations have been driving to. The goal is to achieve Situational Awareness (SA). SA is the correlation and fusion of data from multiple sources that enable decision making. Ideally it will be presented visually through a Common Operational Picture that will facilitate true risk posture understanding and provide information in a format that enables decisions. If the network is lost then the Disaster Recovery (DR) and Continuity of Operations Plans (COOP) come into play. DR focuses on getting the network back up while the COOP is the plan to continue operations without any automation.

As we design systems and networks it is important to understand there are legal expectations of how the network will be protected. These principles are known as due care and due diligence. These should be based on the "Annualized Loss Expectancy" calculations (Vulnerability × Threat × Asset Value = Total Risk then Total Risk × Countermeasures = Residual Risk). This will help determine where the organization is in the security lifecycle: requirements definition, design and develop the protective measures, implement, and validate the defensive solution, operation maintain risk management controls. This will also allow security to be designed into the system rather that bolted on afterwards, something that is always more expensive and less effective.

One of the most effective protection techniques is education designed to alter the users' behaviors. The training must be targeted at the different types of users: leaders need to know how to manage cyber risk, system admins must understand the importance of configuration management and patching, general users need to understand how their behaviors can become vulnerabilities that hackers can exploit, and the cyber security team needs to understand the latest threats and protection tools/techniques. Some useful tools are honeypots, virtual machines, virtual worlds, and live CDs. Honeypots are systems that are deployed with no operational function so any interaction with them causes an investigation. If we install a server with data labeled "senior leaders evaluations and important financial data" it will attract insiders and hackers but as soon as they touch it the SOC will be alerted and quickly react. Virtual Machines (VM) are software-based computers that allow anyone to simulate multiple computers with various operating systems on their computer. This allows them to test hacking from one VM to another. Virtual worlds can be used to conduct training with no travel costs. A popular business-oriented virtual world is Second Life. Finally to boot your current computer as a Linux machine to use some of the tools we have discussed, use a live CD like BackTrack.

WHAT THE THREAT IS AFTER (WHAT WE SHOULD FOCUS ON DEFENDING)

Targeted Capabilities break out the variety of systems, types of information and industries that the enemy is trying to compromise. The major categories are National Critical Infrastructure, Corporate, Personal, and Information Technology (IT) Infrastructure. Critical infrastructure often has aspects of the other categories embedded within it. Corporate information will normally have personal and IT Infrastructure embedded.

National CIP includes: Banking, Law Enforcement, Laws/Legal System, Transportation, Health, Military, Chemical, Energy, State, Emergency Services, Plans, Manufacturing, Commerce, and Aviation. If any of these were not available for even short periods of time, there would be major impacts. The loss of faith in the security of aviation after the 9/11 attacks had secondary economic impacts. The loss of belief in the integrity of our financial systems could cause a run on the banks. If the power grid were to be taken down it would cause both economic and health impacts. The issue is that most of this critical infrastructure is managed by commercial companies that have to balance risk against profit and are generally driven by cost-effectiveness, functionality, and financial gain, rather than security.

Corporate assets such as email accounts, proprietary info/trade secrets, finance records, policy, proposals, and organizational decisions are all of value to the competition. Depending on the nature of the information nation states, criminal organizations, hacktivists, and insiders could all be after different parts of the company.

Personal data like health records and financial information (banking and credit card accounts) are high value targets for insurance companies, criminals, espionage targets, and your personal enemies. If someone wants to target a senior member of the U.S. Military today, finding out as much about the person on the Internet would be the first step. The same could be true of Law Enforcement Agencies that focus on the drug trade. Digital natives are putting more and more personal information on the Web. This information all ties back to two major issues: identity theft and social engineering.

IT infrastructure is a target for two reasons. Hackers may want to use the infrastructure for themselves (i.e., building a botnet) or they want to know what operating systems (i.e., Windows/OS X) and network devices (i.e., VoIP, applications, and specific Cisco devices) are available to allow them to find vulnerabilities. Understanding the architecture or mapping the Web pages could provide insight into how to gain unauthorized access.

SUMMARY

This has been an overview of the threatscape coving the methodology, tools, and techniques used by the different types of attackers and a review of the key parts of the defensive infrastructure employed to protect our systems as well as the general categories of information the attackers are after. These will all be covered in more detail in subsequent chapters but this foundation is intended to help tie it all together. Chapter 15 on Cyberspace Challenges is designed to give an overview of the cyber environment, focused on the challenges. It breaks out the problems in a way that they can be evaluated against each other and facilitates a discussion on prioritization and resource allocation.

The question most often asked after discussing this cyber threatscape is how someone should protect themselves at home. The answer is "safe behaviors!" The basics go a long way such as a firewall, up-to-date antivirus, patching all applications, keeping private and financial data on a removable hard drive that is only connected when in use, and BACK UP valuable data to a place that will not be destroyed if the system is stolen or destroyed. All are mandatory for basic security, but they can all be defeated by poor security practices such as weak passwords, surfing sites known to be hot spots for malcode, and opening emails or accepting invites on social networking sites from someone unknown. While there is no such thing as "security through obscurity" we should strive to not be the "low hanging fruit" that is easily PWNed.

References

[1] Anonymous. UNK [Online], http://www.webutation.net/go/review/anonymousarmy.webs.com.
[2] Brig, Gen. Patterson, LaWarren. Brief on operating, maintaining and defending the Army's global network enterprise. In: Cyberspace symposium, Colorado Springs; 2010.

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