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

Cyber Warfare, Second Edition
http://dx.doi.org/10.1016/B978-0-12-416672-1.00001-5

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

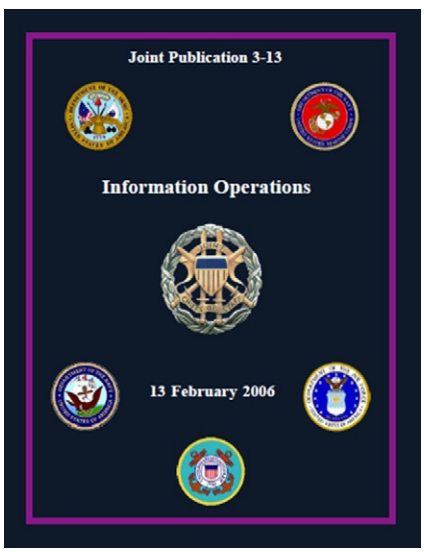

FIGURE 1.1 Cyber or computer network operations falls under this doctrinal manual JP 3-13 information operations [6]. Department of Defense (DoD) joint publication 3-13 information operations 13 February 2006.

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 a*nd *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.

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].