CHAPTER

5

Cyber Warriors

INFORMATION IN THIS CHAPTER

- What does a Cyber Warrior Look Like?
- Differences from Traditional Forces
- Present Cyber Warfare Forces
- Staffing for Cyber War

In looking at the people that are and will be conducting cyber warfare, there are two somewhat distinct areas to examine. At present, many of those that are carrying out such operations are likely to not have been trained from the beginning to do so, due to the relatively recent arrival of the field, and their skills are carried over from other fields. Although this is not a bad thing, and may indeed serve to give them a better and generally more broad technical view, some needed areas will tend to lack focus as the vast majority of the information security field is presently defensively focused.

In the future, as cyber conflicts become more prevalent, and more specifically trained personnel are required, we will need to recruit appropriate people and teach a more focused set of skills to them. In doing so, we will need to look at what these training requirements might be, and the potential consequences of passing on such information.

WHAT DOES A CYBER WARRIOR LOOK LIKE?

The general description of a person engaged in cyber operations may be a difficult order to fill. As the field has only recently begun to become formalized, and most of the personnel are originally from other fields in security and general computing, they have quite a broad range of skills, experiences, and other attributes. We can likely expect this to change in the future as cyber warfare forces become more specifically structured to the task, but at present things are a bit of a hodgepodge.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00005-2

Certifications

Although the world of information security lacks some of the formal credentials of other fields, such as engineering, there is a glut of security credentials, primarily in the form of certifications, to be found, covering nearly any aspect of information security that we should examine. Of primary, but certainly not exclusive, interest, we might commonly find certifications in general information security, penetration testing, and forensics among the groups of people currently conducting cyber warfare tasks. There are, of course, also people conducting these tasks that have no certifications at all.

There are three main types of certifications to be found across the technical computing industry: those that are vendor neutral and sponsored by a collective of organizations, those that are vendor neutral and put forth by a single organization, and those that are vendor specific and launched by the vendor itself.

In the general information security field, the single certification that holds the most weight at present is the Certified Information Systems Security Professional (CISSP®) from the International Information Systems Security Certification Consortium (ISC)²®. The CISSP®, although considered to be a management certification, has become the "gold standard" against which security professionals are weighed, and without which a job above entry level might be very difficult to find in the security industry. Also of note in general information security certifications are a variety of offerings from the SysAdmin, Audit, Network, Security (SANS) Institute, with certifications provided by Global Information Assurance Certification (GIAC), the certification body associated with them, as well as the offerings from the Information Systems Audit and Control Association (ISACA).

In the penetration testing field, certifications are somewhat fewer and farther between. Again from SANS/GIAC, the GIAC Certified Penetration Tester (GPEN) certification has become well known in the last few years. Although a solid certification, the GPEN test does not include a hands-on assessment, which raises criticism from some regarding what exactly is being tested for this very results-oriented specialty of the security field. A relative newcomer to the penetration testing certification cadre, and one that had gained a considerable amount of attention, is the Offensive Security Certified Professional (OSCP), a certification created by the same group that develops the BackTrack pen testing Linux distribution. The OSCP test is offered online and consists largely of being able to successfully attack and exploit a number of systems in order to retrieve specified information, a scenario much more closely matched to what we might find in a cyber warfare operation.

In the forensics field, we can again find several offerings from SANS/GIAC, in a few different subspecialties of forensics.

We can also find several offerings that are vendor specific, often from forensics software vendors, such the EnCase Certified Examiner (ENCE) certification from Guidance Software, the makers of the commonly used EnCase forensic toolset.

While this by no means represents a complete list of all of the certifications, nor of specializations, that we might find in information security professionals, and in those capable of conducting cyber warfare, it is a relatively representative sample.

TIP

Many security classes and certifications come with a very high price tag, including those from SANS. For those willing to put in a little bit of work in exchange, SANS offers a workstudy program that allows training classes to be attended for a considerably reduced cost. This renders the road to certification considerably more accessible, at least from a monetary perspective. Further information can be found at http://www.sans.org/security-training/volunteer.php.

Education and Training

In general, those that work closely with information security in general, or in the cyber warfare arena specifically, tend to be rather well educated and trained. Outside of lower-level jobs, entry into positions in these fields is not always easy and tends to be rather competitive. We will generally find that such people are, in general, relatively well educated to begin with, and undergo continual rounds of training, attend conferences and seminars, and generally try to keep their skills as current and sharp as possible.

Education

Education, in the sense of formal university degrees, in the information security field can vary widely, although it does tend toward the higher end of the scale. In general, studies that have been done on information security professionals show that around half of them have at least a bachelor's degree, with some relatively large fraction of that group having a master's degree as well. Additionally, we will find a very small percentage with terminal degrees [1]. Such degrees, although largely technical in nature, also expand to include the arts, history, and many other non-technical areas. Technical degrees such as those in computer science, computer engineering, information technology, information assurance, and others in the same vein have some direct applicability to cyber warfare, although such academic knowledge not tempered with practical experience is of considerably less utility.

At present, a large portion of those conducting cyber warfare operations in the United States are current or former military, and of those that are or were commissioned officers, a certain number will have come through one of the military academies. Defense contractors, who are often providing the actual personnel for such efforts, tend to favor former military due to skill set and clearance issues. In addition to the benefit of the college degree earned at the academy for their particular branch of military service, such people will also have gained knowledge of strategy and tactics as a part of their educational process, knowledge that could be quite useful in conducting cyber warfare operations. In particular, those that have been through such schooling in the last few years may very well have had educational experiences that spoke specifically to cyber warfare. This dimension of warfare has recently come considerably closer to the forefront in military circles, and this focus is reflected in the content at many military academies [2].

Also worthy of mention is the National Security Agency (NSA) Center of Academic Excellence (CAE) institutions. The NSA reviews the information security curriculum and the credentials of the school in question, and makes a determination on the quality of the security-related programs that are offered by school. The CAE is awarded when a school meets or exceeds the criteria for information security training that have been set by the NSA.

Training

A very large portion of those in the information security and cyber warfare fields go through quite a bit of effort to keep their training and skills current. In this particular profession, being linked so closely to technology, and, in particular, to keeping technology secure, means that keeping up on training and staying abreast of events is vital to staying current. This is generally done by attending formal training sessions, going to conferences, watching the news outlets that are specific to security, reading new books and papers that come out, and other similar activities.

In the world of formal security training, there are a large variety of options to choose from, but most of them cover the same relatively limited pool of information. The focus of such offerings changes with the focus of the industry, so there are sure to be a glut of classes for whatever the hot topic is at any given time. At present cyber warfare is the hot new thing in the security industry, so many training vendors are pushing penetration testing, the nearest thing to directly address the topic. Outside of a few vendors that produce unusual training, most such classes will fit into penetration testing, incident handling, digital forensics, law, auditing, or development relatively neatly. In such classes, we will find often our cyber specialists in attendance.

One of the other main avenues of keeping up to date with the security and cyber fields is to attend the various conferences, seminars, and other similar events that are available in a near continuous stream. These events can arrive as everything from very large general security conferences to very specialized and more exclusive events on particular sub-topics. In the last several years, we have seen quite a few more events that are specific to cyber warfare; however, these are often sponsored and attended almost entirely by military and government organizations and often do not enjoy the attention of the general public.

Experience and Skills

The experience and skills held by those in cyber operations can be quite wide and varying, but often maps well to several of the general information security and computing fields. If we make a fairly broad generalization, we can break such skill sets down into reconnaissance, offensive, and defensive skills.

Reconnaissance skills such as network traffic sniffing, packet analysis, network and system mapping, forensics, reverse engineering, binary analysis, and other such capabilities allow us to examine the infrastructure, systems, traffic, and often data of those that oppose us on the cyber battlefield. Such skills are commonly used in the troubleshooting of systems, applications, and networks, although usually with a slightly different focus. We may find people with such experience working in system administration, development, network engineering, and security roles.

Offensive skills are somewhat more specific and focused in the direction of attack and, as such, do not overlap with quite as many non-security fields, although they still do to some extent. The set of skills found in hackers (ethical or otherwise) and penetration testers maps almost directly across, although with a slightly different focus and rules of engagement. The skills of fields such as network engineering, development, and others can also be of use here by changing the goals from keeping infrastructure, systems, and applications running to taking them down.

Defensive skills are already rather prevalent in the computing industry in general, although generally not with the sole focus of withstanding a concentrated cyber attack from a determined enemy with the resources of a nation state to back them. These standard skills are found in system administration, penetration testing, network engineering, and many other common areas. Although they are skills found in most IT departments, we are less likely to find individuals that have the particular focus of defending against a large scale attack, outside of a few major providers or hosting services that have been through such trials already. For example, Akamai, a company that provides, among other things, hosting services for many large companies, and is attacked quite regularly.

As we have noted, the skills used to conduct cyber warfare are not uncommon ones, but they have a different focus than their industry counterparts. When looking for those that are experienced in the cyber warfare area, we are unlikely to find the very specific skills that we are looking for, unless the person in question is already working in the cyber area, conducting research, or a related field. The better candidates for such positions will have a broad variety of technical skills and a good general understanding of hacking, networking, development, system administration, and other similar areas, and an ability to be creative and thing outside of the box. Although specialists do have their place, they can be blind to particular areas and may be better focused on single tasks.

DIFFERENCES FROM TRADITIONAL FORCES

In selecting candidates for cyber warfare operations, we may find, and the U.S. military has found, that those suited to this particular task may differ in some rather significant areas from those that are traditional in fighting forces the world over. Although we may desire a certain set of qualities from someone for taking a hill or shooting someone a long distance away, these same qualities may not be significant for conducting cyber warfare.

Age

Age can be significant in several ways for traditional fighting forces. We may want our troops to be young enough to be in or near their physical prime, so that they can withstand the rigors of combat, but not too young or too physically underdeveloped. We are also less likely to value those that are of a more advanced age, due to the physical concerns and lessening of strength and stamina past a certain point.

In the world of combat on a largely logical level, many such concerns vanish entirely. When conducting operations from behind a computer screen, measures of age-related physical strength and fitness become exponentially less important, if they are a consideration at all.

On the other side of the coin, mental factors such as maturity, intelligence, and problem-solving skills become dramatically more important in this type of engagement.

The reduced reliance on attributes related to age gives us a considerably larger potential pool of candidates from which to select. We can potentially recruit, where other factors permit, from a range much younger or older than would normally be considered for operations of a militaristic nature. We still need to consider health factors, maturity level, and other such items, when making such selections.

Although this could be considered a positive thing from a personnel perspective, we would also need to consider the psychological effects that having "kids" or "seniors" presents in such conflicts. Even away from physical frontlines and out of danger of immediate physical harm to their persons, we might see a variety of effects on other segments of our fighting forces, and a certain amount of backlash that might be associated with using such candidates, just as we have seen with discussions in the introduction of other groups potentially not conforming to the military image, namely homosexuals. Nonetheless, we must maintain an awareness of possible candidates, regardless of the ageism present in many modern societies.

Attitude

When considering the ideal type of mind that we may seek out to conduct cyber warfare operations, a few attributes present themselves: creative, intelligent, good problem solving skills, independent, and other similar terms. Unfortunately, or perhaps fortunately, depending on perspective, these types of attributes do not generally produce people that tend to follow rules well, or possess any willingness to follow strong authority figures. People, of course, vary greatly and in unexpected ways, so this will by no means be a universal issue, but it will be prevalent enough to pose some difficulty when attempting to attract large numbers of people with such qualities, and will need to be accounted for when attempting to do so.

Additionally, as we discussed above when we covered the broadened age range that we have to select from when assembling a non-physically oriented force, attitude issues may accompany those at either end of the age spectrum. For those that are at the younger end of the spectrum, we may encounter issues such as maturity and impulse control. At the older end of the spectrum, we may have societal issues involving a perceived lack of respect of deference from those that are considerably younger. Again, these types of problems can be highly situational and vary greatly from one individual to the next, but definitely need to be accounted for and prepared for.

Physical Condition

The physical condition of dedicated cyber warfare forces, security professionals, and those that work with computers for a living, in general, tends to be very different than that of the membership of the militaries and other fighting forces in most countries. While generally good physical fitness, granting the ability to move quickly over long distances, engage in physical combat with enemy forces, and other such strenuous activities, may be very valuable in traditional combat, this is not necessarily the case when seeking to conduct cyber warfare.

In the case when the truly valued assets of our cyber warrior revolve largely around mental abilities, creativity, technical skills, and the ability to sit in a chair for long periods of time, all

the while tracking multiple activities on a series of displays, physical fitness may tend to take a back seat. Although it is obviously desirable for our best and brightest to be fit enough to allow them to function relatively normally, some are of the opinion that such traditional military measures of physical performance, such as timed runs around a track are not necessarily applicable. On the other side of the discussion is the potential for cyber forces to be deployed in an area where a traditional ground/air war is being carried out. In this case, it may be vital for such forces to be physically fit.

It is the nature of modern conflicts involving new and complex technologies that will force a paradigm change in the way that a soldier is viewed. Even in traditional warfare, we can see a surge of new technologies, such as the use of unmanned and remotely piloted drone aircraft, that usher in a wave of chair-bound and technically savvy operators, having many of the same skills, background, and characteristics as our cyber warriors.

Although this attitude regarding the physical fitness of tech workers is commonly accepted in the civilian world, it is one that is sure to be a very difficult change to internalize in many organizations of a military and governmental nature. Although such changes may not be commonplace at this time, they are sure to become considerably more so in the future.

Credentials

An interesting anomaly in the security world, and in the world of technology in general, is the importance of credentials, or lack thereof, depending on the given situation. In many other disciplines that depend heavily on complex domain expertise, such as civil engineering or medicine, the ability to legally practice such skills is tightly regulated, and justifiably so. We do not want to see a bridge erected or an appendix removed by someone who has a set of knowledge bounded by a weekend with a "<skillhere> for utter morons" book. In the commercial security field, we can often see examples of exactly this, and the world is awash with self-proclaimed experts in this area.

In some cases, primarily in military and government, we can see some steps that have been taken to avoid such situations. An excellent example in the U.S. military can be found in Department of Defense (DoD) Directive 8570.1, commonly referred to as DoD 8570, or just 8570. DoD 8570, in a nutshell, requires that those in the direct employ of the DoD who are performing information assurance-related functions be trained and certified to be capable of carrying out their particular role, and that certification for these functions are carried out by a vendor on a relatively short approved list. The vendors that are on the approved list also enjoy a certain amount of fame in the civilian world, as they presumably measure up to a higher level of quality for having been so included. The present, as of this writing, table of approved certifications for various DoD career fields and levels can be seen in Table 5.1 [3].

The interesting dichotomy in this situation is that certification does necessarily equate to skill or knowledge, and lack of certification is not always a good indicator of lack of knowledge or skill. When selecting candidates for cyber warfare, unlike picking a doctor to remove our appendix, we cannot presently afford to immediately discard those that do not possess a given certification in the security field. In the future, we may see a more closely regulated security industry, but at present, we may be as likely to find our best prospects waiting tables or arranging flowers as anywhere else.

TABLE 5.1 DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE	GSEC	CISA
Network+ CE	Security+ CE	CISSP (or Associate)
SSCP	SSCP	CASP
		GCIH

IAM Level I	IAM Level II	IAM Level III
CAP	CAP	GSLC
GSLC	GSLC	CISM
Security+ CE	CISM	CISSP (or Associate)
	CISSP (or Associate)	
	CASP	

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	CISSP (or Associate)	CISSP—ISSEP
CASP	CASP	CISSP—ISSAP

CND Analyst	CND Infrastructure Support	CND Incident Reporter	CND Auditor	CND-SP Manager
GCIA	SSCP	GCIH	CISA	CISSP—ISSMP
CEH	CEH	CSIH	GSNA	CISM
GCIH		CEH	CEH	

PRESENT CYBER WARFARE FORCES

Although the idea of formal cyber warfare forces is a relatively new one, only going back a few years, many countries and organizations have at least taken steps in that direction.

WARNING

Due to the present volatile situation in the world of cyber warfare, information regarding the capabilities of various countries is rapidly changing. It is not unusual for government and civilian agencies dealing with cyber issues to be restructured, merge into and split from each other, and disappear or appear very quickly. The information in this section is subject to change.

In a few cases, large organizations have sprung into existence virtually overnight, even if they are not entirely operational and ready to take on a large conflict. Even the question of what exactly constitutes operational is somewhat up in the air, as many of these units and organizations have not been tested under live circumstances.

Looking at Figure 5.1, we can see that even when only accounting for the major players in the cyber warfare arena, we still have a large percentage of the globe that could potentially be involved in such a conflict.

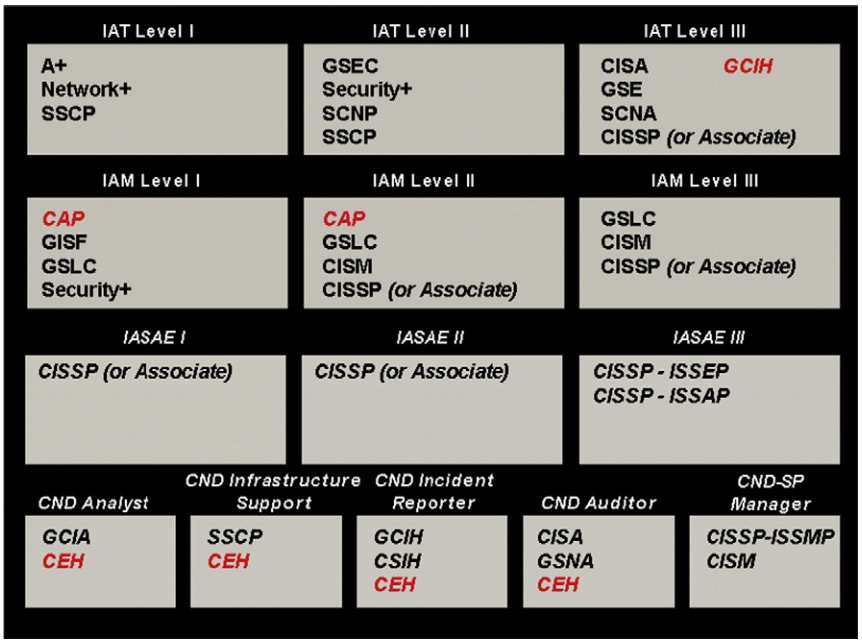

FIGURE 5.1 The major forces in the cyber warfare arena.

U.S.

The U.S. government has one of the more complex groupings of cyber warfare forces, at least on paper. In reality, though these organizations and agencies exist, they are not all staffed, operational, and completely ready to carry out such operations on any large scale.

U.S. Cyber Command

The U.S. Cyber Command (CYBERCOM) is a unified command under U.S Strategic Command (STRATCOM), composed of units from the Army Cyber Command, the Fleet Cyber Command (10th Fleet), the 24th Air Force, and the Marine Corps Forces Cyberspace Command [4]. The seal of CYBERCOM can be seen in Figure 5.2 [5].

CYBERCOM is headed by the Director of the National Security Agency (DIRNSA), who serves both roles, and is assisted in technical matters by the Defense Information Systems Agency (DISA). The Cyber Command is specifically responsible for the protection of DoD networks only, leaving the protection of civilian networks up to the Department of Homeland Security (DHS) [6].

China

The public face of cyber warfare in China rests with the People's Liberation Army (PLA), although the specifics are a bit sketchy on exactly the composition and duties of cyber warfare units within the PLA are. It is believed that the majority of such capabilities lie within

FIGURE 5.2 The seal of the United States Cyber Command.

the General Staff Department (GSD), 4th Department, GSD 3rd Department, several of the Technical Reconnaissance Bureaus (TRB), and the Information Warfare Militia Units [7].

NOTE

As we discuss the cyber capabilities of the various countries in this section, please note that they are in no particular order and their positioning in the chapter does not indicate strength, ability, or any other factor.

Also to be considered are the informal, or at least not publically recognized, groups of hackers, hacktivists, malware authors, cyber criminals, and other such similar elements that are frequently discussed in the media. Although we might suppose that all of the attacks attributed to China are not actually sponsored by the state, if they originate from the country at all, there may be at least some element of truth present here. The large population of China also equates to a large number of potentially unsecure systems that could be used as attack platforms. We will discuss the attribution issue in Chapter 9 and criminals and criminal organizations at greater length in Chapter 11.

Russia

It is clear from the events in Estonia and Georgia that we discussed in Chapter 1, that Russia has a strong capability to conduct cyber warfare. Presently these capabilities are housed in the Federal Security Service of the Russian Federation (FSB), the Federal Guard Service, and the General Staff [8]. Until it was abolished in 2003, the Federal Agency for Government Communications and Information (FAPSI) solely handled such matters in Russia [9].

France

The cyber warfare capability of the French springs from the French Network and Information Security Agency (ANSSI), which is an organization under the Secretary General for

National Defense (SGDN) and exists to "detect and early react to cyber attacks" [10]. This organization is, as are those of many countries at this point, relatively new, having been in existence for only slightly over a year at the time of this writing.

Israel

As with many other aspects of warfare, Israel is and has been for some time very proactive in the area of cyber warfare. Israel reportedly has had at least some cyber warfare capability since the early 1990s, and these capabilities have matured and evolved over time. In 2002, a special unit of the Israel Security Agency (ISA) was charged with matters of defense against cyber attacks. At present the task of cyber warfare operations appears to be somewhat of a contested split between the C4I (command, control, communications, computers, and intelligence) Directorate of the Israel Defense Force (IDF) and Unit 8200 (signals intelligence) of the Directorate of Military Intelligence which is commonly known as Aman [11].

Brazil

In Brazil, a country that is no stranger to cyber crime issues, the responsibility for issues related to information security lies with the Institutional Security Cabinet (GSI), which ultimately acts through other related organizations such as the Ministry of Science and Technology, Ministry of Communications, and the Brazilian Network Information Center [8]. The technology industry in Brazil is evolving quickly, so we will likely see a more formalized organization or set of organizations here in the very near future.

Singapore

In Singapore, the Singapore Infocomm Technology Security Authority (SITSA), a division of the Internal Security Department of the Ministry of Home Affairs (MHA) is responsible for securing Singapore against cyber attacks [8]. SITSA, as with many other such agencies, is relatively new and has only existed for slightly over a year as of this writing.

South Korea

Although the stance on cyber warfare in South Korea was previously very disjointed and was divided among a variety of government agencies numbering into the dozens, in 2009, they began an effort to consolidate and standardize the agencies that would be responsible for handling such matters. At present the Korea Internet & Security Agency, composed of the former Korea Information Security Agency (KISA), National Internet Development Agency of Korea (NIDAK), and the Korea IT International Cooperation Agency (KIICA) appears to now be officially responsible for cyber operations [12].

North Korea

The capability of the Democratic People's Republic of Korea (DPRK), otherwise known as North Korea, to conduct cyber warfare is questionable, but may actually exist, at least

according to the South Korean intelligence services. Two North Korean educational institutions, Mirim College and Moranbong University, appear to exist for the nearly sole purpose of producing experts in espionage and warfare, of which cyber war is reported to be at least a portion. Additionally, a unit of the Korean People's Army (KPA), dedicated to cyber warfare, is rumored to exist [13]. Outside of a few attacks on South Korea which were tenuously attributed to North Korea, examples of such capabilities are thin indeed.

Australia

In Australia, the Cyber Security Operations Centre (CSOC), under the Defense Signals Directorate (DSD), was launched in 2009, and populated with personnel from the DSD, the Defense Force, the Defense Intelligence Organization, the Federal Police, and the Australian Security Intelligence Organization. The CSOC is responsible for cyber matters pertaining to government computer systems. For civilian systems, the responsibility falls to CERT Australia [14].

Malaysia

In Malaysia, the responsibilities for cyber warfare are spread over several government agencies. The Malaysian Communications and Multimedia Commission (MCMC) acts as a coordinator and has responsibility for ensuring the overall well-being of the network as a whole. The Police Cyber Crime Unit is responsible for preventing and investigating cyber crime. The Ministry of Science, Technology, and Innovation (MOSTI) is responsible for cyber defense and security, and the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) is responsible for both government and civilian CERTs and monitoring cyber threats [8].

Japan

In Japan, the Information Security Policy Council (ISPC) and the National Information Security Center (NISC), both under the Cabinet Secretariat, are largely responsible for cyber issues. The ISPC focuses on developing and reviewing security policies and strategies, while the NISC handles implementations. Also under the Cabinet Secretariat, the National Police Agency (NPA), is responsible for maintaining computer and network security and investigating cyber incidents. The interface between the public and government cyber concerns lies with the Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response, or CEPTOAR [7].

Canada

In Canada, the Canadian Cyber Incident Response Center (CCIRC) is responsible for monitoring cyber threats to the Canadian network infrastructure. The CIRC falls under Public Safety Canada, the Canadian equivalent to the Department of Homeland Security in the United States. Several agencies are involved in responding to cyber threats and incidents including the Canadian Security Intelligence Service (CSISS), Communications Security Establishment Canada (CSEC), and the Canadian Department of National Defense (DND) [7].

United Kingdom

In the United Kingdom, two main agencies are responsible for cyber issues, the Office of Cyber Security (OCS) and the Cyber Security Operations Centre (CSOC). OCS provides strategic leadership across the whole of the government, while CSOC provides monitoring and coordinates incident response. Additionally, the Centre for the Protection of National Infrastructure (CPNI) runs a CERT for responding to attacks [8].

Other Countries with Cyber Forces

Many other countries currently field, or are in the process of standing up, cyber forces. Some countries may not, at this point, have any significant resources devoted, and others may not be advertising their capabilities. At the time of this writing, considerable confusion and wild speculation in the media and in the industry do not help to make the cyber landscape any more clear. In addition to the countries mentioned above, the following are known to have some presence, but this is by no means an exhaustive list and exact capabilities are not clear [8]:

- Austria
- Belgium
- Estonia
- Finland
- Germany
- Hungary
- India
- Iran
- Italy
- The Netherlands
- New Zealand
- Norway
- Poland
- Spain
- Sweden
- Switzerland

Corporate

Given the increased focus on cyber warfare in the last few years, and the current focus on the topic in both government and industry, a large number of companies have, predictably, become involved in cyber warfare in one fashion or another. In the world of companies that primarily focus on defense contracts we can find the following non-exhaustive list of companies [7]:

- BAE Systems
- Boeing Integrated Defense Systems
- Booz Allen Hamilton
- General Dynamics Corporation

- GreyLogic
- Lockheed Martin Corporation
- ManTech International Corporation
- NetWitness Corporation
- Northrop Grumman Corporation
- QinetiQ Group Plc
- Raytheon Company
- Science Applications International Corporation (SAIC)
- TASC, Inc.
- Thales Group

The list of companies below, also not exhaustive, does not primarily focus on the defense market, although we can almost certainly find most of them in the market to a certain extent [7]:

- F-Secure Corporation
- iDefense
- Kaspersky Lab
- McAfee Inc.
- Microsoft Corporation
- PGP Corporation
- Spirent Communications
- Symantec Corporation

In addition to these companies, we can find thousands of others that have similar foci, products, services, and customers. The market for cyber-oriented offerings is very rich at present, and promises to be so for several years to come, so we are sure to see more entries as time passes.

Criminal

In addition to the various countries and organizations that we discussed above, we must also consider the criminal elements in our list of cyber warfare forces. These can range from the lowest spammer annoying us with promises to enlarge various portions of a man's anatomy, to identity thieves that have managed to parlay stolen information into tens of millions of dollars in funds, to botnet operators that are capable of disrupting the network operations of large corporations or small countries.

Such criminal elements are not as easy to define and point out as the formal cyber warfare forces of a country, but they can be every bit as powerful, and are not bound by the same sets of rules that other forces might be, which can make them very dangerous. We will discuss such elements in greater depth in Chapter 11.

STAFFING FOR CYBER WAR

Given the current situation in which most countries in the world are arming themselves for cyber warfare, there is a large demand around the globe for people with the skills to carry out such operations. In the United States, many of the defense contractors that actually provide

the staff for such roles are constantly recruiting, and doing so in such a fashion as to catch the attention of a younger and more technically savvy group of people. Likewise, many military organizations, such as those in the United States and China, are actively recruiting for such positions, once again, with a large target on the backs of younger and potentially more technically able recruits. As we discussed in the "Differences from Traditional Forces" section earlier in the chapter, though age may not be a factor in determining the capacity of a person to carry out cyber operations, technical skill certainly is. The general perception appears to be that such skills can be found to a greater degree in younger people or digital natives.

Particularly given the high level of demand, there is a shortage of people with the technical skills needed to step directly into roles such as these [15]. Defense contractors tend to favor, if not require, potential candidates that have prior military experience. Military recruits have the hurdle of going through rigorous and time-consuming training processes before they can even begin to learn the technical specialties that would make them valuable to such operations. Conversely, if such skills are not used and maintained, they will quickly become outdated.

In short, many countries are in a crunch for qualified people to man these positions, and they may have to alter their current standards to get them. Although this may change in the future, especially if the demand for cyber capable candidates keeps up or increases, for now the situation in the staffing world is rather tight.

Sources of Talent

Sources of sufficiently talented people for recruiting into cyber warfare efforts could potentially come from a wide variety of areas, but a couple present themselves as the most likely sources, namely hacking competitions and schools. Although groups from the two of these may overlap, they ultimately tend to produce a slightly different variety of skills and experiences.

Hacking competitions often referred to as Capture the Flag, or CTF, events value practical skills almost entirely. The general goal of a CTF competition is to exploit one or more machines in order to gain information to either reach the end goal itself, the flag, or to gain information to exploit additional machines with the end goal in mind.

NOTE

There are a large number of such competitions, both inside and outside of the United States, including the National Collegiate Cyber Defense Competition,[a] the Cyber Defense Exercise[b] (CDF), the Defcon CTF[c] competition, Netwars,[d] and Cyber Patriot High School Cyber Defense Competition.[e]

[a] http://www.nationalccdc.org/

[b] http://www.nsa.gov/public_info/press_room/2010/cyber_defense.shtml

[c] http://www.defcon.org/

[d] https://netwars.info/

[e] http://www.highschoolccdc.com/

In academic settings, attention is often more focused on learning the basics and theory behind information security thoroughly, with considerably less emphasis on the practical implementations. Where such situations are discussed, they are often limited to purely defensive topics. Of course there are some schools that are exceptions to this rule, but they are not common.

Ideal candidates are those that have both a deep understanding of the principles of information security, as well as practical knowledge and experience in the specific areas in which they will be working. Such people are not only somewhat more difficult to come by, but chances are that they will either be employed in the field already, or will be actively recruited for their somewhat unique attributes.

Training the Next Generation

Training the next generation of those who will carry out cyber warfare is an interesting prospect. Not only are we training those that are new to the field, but also retraining existing personnel to cope with newer paradigms. Although we can presently muddle through, to a certain extent, by depending on the small core of capable forces that do exist, we are largely depending on being able to retune the skills of those security professionals that already exist in a few small fields in the information security industry.

Currently when such security personnel fail at their jobs, we see something along the lines of a large breach of Personally Identifiable Information (PII), such as contacts information, financial information, medical data, and the like, often closely followed by a rash of identity thefts.

Although such occurrences are unfortunate and can certainly lead to no small amount of financial and emotional trauma for the victims, they pale in comparison to the damage that could be caused by a well backed attacker intent on causing physical harm by attacking critical infrastructure and systems. These attacks have the potential to be orders of magnitude worse if targeted at power infrastructure systems, safety systems, distribution networks for food, and the like.

To train specifically to carry out and defend against an actual cyber conflict, our training focus will need to shift in order to be able to cope with the change.

The Training Paradigm

One of the realities of being closely linked to a constantly changing slate of computing technologies is that change comes at a lightning pace. Although we have yet to see cyber warfare on a large scale, we see a relatively constant stream of small conflicts between various countries, criminal organizations, corporations, and individual players. The lack of a large altercation has less to do with the technology to carry it out not being present, and more to do with a determined attacker having yet to step up to carry out such an attack. In other words, we could find ourselves embroiled in a true cyber war at any point. The prospect of this begs the need of an immediate influx of new blood to be trained for just such an occasion.

Although the need for such training in the immediate future is clear, the practicality of being able to functionally provide such knowledge may be more difficult than it might immediately seem. The U.S. does have a number of commercial training institutions that presently teach on more sedate, but similar, topics, and they presently provide the majority of such

training for personnel, civilian, government, or otherwise. These training venues would need to not only retool their training in a much less commercially and perhaps publically, palatable direction, but might also need to keep such training out of the hands of the general public. The necessity might arise to move the delivery of such training inside of the organizations where it would be used, which would require a rather large paradigm shift in the training industry as well.

Teaching the Needed Skills

As we discussed earlier in the chapter in the "Experience and Skills" section, the chief skills required to conduct cyber warfare are reconnaissance, attack, and defense. In the information security world at present, the gross skills that comprise what we need for reconnaissance and attack already exist to a large extent.

Defense, unfortunately, is an area in which most organizations are severely lacking. True defense against concerted attacks, such as large scale Distributed Denial of Service (DDoS) attacks, at this point usually revolves around ignoring the attack in some fashion until it goes away, either by bringing redundant systems online, or some similar strategy. In order to successfully withstand attacks on the scale that we might see in a cyber conflict, we will need to develop new methods of defense and be allowed the freedom to use existing ones. An excellent example of the issue of defense at present is that of the rampant and unchallenged use of botnets. The major issue behind the botnet problem lies in the fact that the simple steps that need to be taken to dismantle a botnet are illegal in many countries. This is largely due to the unauthorized intrusion onto the systems that comprise the botnet that would be required to take it down. Because the skills required to employ such methods of defense are not generally allowed to be used outside of research labs, these skills are not well developed. When examining the skills required to conduct cyber warfare, many such examples present themselves.

Issues in Training for Cyber Warfare

When looking to train large groups of people to conduct cyber warfare, we also need to look to the potential consequences of doing so. At present, the majority of formal training that is oriented in the direction of hacking, our current closest analog to cyber warfare, is firmly directed at what is called "ethical hacking." Ethical hacking, red teaming, and penetration testing are often interchangeable terms, and tend to point at the same set of carefully carried out, with advanced permission being granted, attacks that are intended to root out (pun intended) vulnerabilities so that they can be mitigated before a malicious attacker can find them. This type of training is fairly universal and is provided to those in the corporate world and those in the government world alike. Such training is often expensive enough to be out of the reach of those that do not have the backing of a corporation or government entity.

When we shift our training slightly to focus on cyber warfare instead of ethical hacking, we move somewhat away from the carefully regulated world of ethical hacking, and we almost certainly would not be granted the permission of the party being attacked. In such an environment, the definition of the party conducting the attack becomes almost entirely a matter of perspective. The attacking party may see such an operation as contributing to the defense of their country in both a physical and logical sense, but the opposing party may see such actions

as those of a malicious attacker. In this way, one potential viewpoint of training personnel for cyber warfare is also training them for cyber crime.

With traditional forces, when the conflict is over, or when they have been released from their duties, the harm that can come from their training is relatively minimal. They will likely have not been allowed to depart their service with any form of advanced weaponry, although they will still be in possession of the strategic and tactical knowledge in which they were trained. They will also have the benefit of the ingrained lessons of discipline that have been drilled into them over a period of time. These factors will generally allow them to be a normally functioning member of society.

In the current theoretical world where large numbers of individuals have been trained in the conduct of cyber warfare, the peaceful reintroduction of combatants into society may not necessarily be the case. In such circumstances, the mitigating factors that we looked at for traditional forces may not be present at all, or may be lessened.

In cyber warfare, stripping our troops of weaponry when they leave our service may be a difficult prospect. We can certainly attempt to remove their direct access to the systems that would facilitate such attacks, but we will have likely also trained them specifically to subvert such attempts at access control. Even in the case of being able to successfully remove access to such resources, the tools with which cyber warfare is carried out are not (presently anyway) unusual by any means. More often than not, such tools are free, open source, and easily available to the public. Additionally, if we have done a proper job in our training, we should be producing people sufficiently skilled as to be little inconvenienced by the removal of a few specific tools.

Speaking to the issue of discipline ingrained over time by exposure to strict training, we have discussed some of the differences in those that would be suited to cyber warfare from those that are ideally suited to be soldiers in a traditional conflict. As one part of the issue, we may find ourselves surrounded by people that are naturally questioning authority, are independent thinkers, and are particularly bright. On the other hand, the need for such capabilities is now, and lengthy training may not be an option. The combination of the two of these sets of factors does indeed have the potential to be troublesome moving into the future.

SUMMARY

In this chapter, we discussed cyber warriors. As cyber warfare is a rapidly developing field, we covered both the existing forces, and talked about what might come in the future.

We talked about what those working in the cyber field presently look like from the standpoint of education, training, certifications, and experiences. Because this is a relatively new field, we looked at how such skills overlap several other related fields. We also discussed the sources that such skills might come from, and how they are maintained.

We covered what the differences between those that are selected for traditional warfare and cyber warfare might be. Here we talked about how factors such as age, attitude, physical condition, and credentials might apply differently to people fighting from a chair rather than a traditional ground war.

We discussed the present cyber warfare forces in countries around the globe. The list of countries that have formal cyber warfare forces is a relatively short one, but many other

countries are developing such capabilities. We also covered how corporate and criminal organizations fit into the picture.

Lastly, we discussed training the next generation of cyber warriors. We covered the training paradigm and how a change might be required to support a true cyber war. We discussed the skills required for cyber warfare and how they differ from the related skills that now exist. We also covered the implications of training people for cyber war and later releasing them into society.

References

[1] Frost & Sullivan. THE 2013 (ISC)2 Global information security workforce study. s.l: (ISC)2®, https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf; 2013 [accessed 04.04.13].
[2] Witte B. Military academies teach more cyberwarfare. Navy Times, http://www.navytimes.com/news/2010/03/ap_cyberwarfare_030810/; 2010 [accessed 04.04.13].
[3] Assistant secretary of Defense for networks and information, integration/Department of Defense chief information Officer. DoD 8570.01-M Information assurance workforce improvement program incorporating change 3, January 24, 2012. s.l.: United States Department of Defense, http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf; 2012 [accessed 04.04.2013].
[4] U.S. Strategic Command – Fact Sheets. United States strategic command, http://www.stratcom.mil/factsheets/cc/; 2010 [accessed 04.04.13].
[5] United States Cyber Command. cybercom_seal_large1. United States cyber command, s.l.; 2010.
[6] Deputy Secretary of Defense William J. Lynn, III. Remarks at the defense information technology acquisition summit; 2009.
[7] Visiongain. Cyberwarfare market 2012–2022; 2011.
[8] Buckland BS, Schreier F, Winkler TH. Democratic governance challenges of cyber security; 2010.
[9] Pike J. Federal Agency for Government Communications & Information (FAPSI). FAS intelligence resource program, http://www.fas.org/irp/world/russia/fapsi/index.html; 2003 [accessed 04.04.13].
[10] About ANSSI. Agence Nationale de la sécurité des systèmes d'information, http://www.ssi.gouv.fr/site_rubrique97.html; 2013 [accessed 04.04.13].
[11] Ben-David A. Israel Is serious about cyberwarfare. Aviation week, http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_03_29_2010_p56-212531.xml; 2010 [accessed 04.04.13].
[12] Korean Internet & Security Agency. Korean Internet & Security Agency, https://www.kisa.or.kr/eng/main.jsp; 2013 [accessed 04.04.13].
[13] Mecca for North Korean Hackers. Daily NK, http://www.dailynk.com/english/read.php?cataId=nk01500&num=5161; 2009 [accessed 04.04.13].
[14] Defense Signals Directorate. The cyber security operations centre. Defense signals directorate, http://www.dsd.gov.au/infosec/csoc.htm; 2013 [accessed 04.04.13].
[15] Evans K, Reeder F. A Human Capital Crisis in Cybersecurity. Center for strategic & international studies, http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity; 2010 [accessed 04.04.13].