© Rodolfo Clix/Dreamstime.com

CHAPTER 2

Targets and Combatants

THE HISTORY YOU LEARN IN SCHOOL is filled with stories of military victories and losses. People immediately conjure up images of armies marching off to fight when the word *war* is mentioned. Over thousands of years of documented human warfare, people have become used to identifying a variety of traditionally accepted military targets. These include military bases, vehicles, groups of soldiers, and infrastructure that supports military operations. Many of the same targets exist in cyberwarfare. An enemy can attack strategically important military units, facilities, infrastructure, vehicles, and, more recently, the control systems for drones.

The variety of targets and combatants who may participate in cyberwarfare is broad. Further, many of the countries considered to have significant cyberwarfare capabilities typically do not make public their doctrines for cyberwarfare. This chapter discusses concepts that expand the ideas of cyberwar beyond those currently accepted as part of U.S. cyberwarfare doctrine. It explores the wider potential boundaries of a changing form of warfare. As you read this chapter, keep in mind that U.S. cyberwar doctrine currently defines cyberwarfare to include three elements: computer network attack (CNA), computer network defense (CND), and intelligence gathering. The shifting boundaries of cyberwar—and the interaction between other parts of information operations and CNA, CND, and intelligence activities—mean that to fully explore targets and combatants, you need to look beyond the current scope of U.S. doctrine.

Cyberwarfare also expands the boundaries of warfare beyond the traditional targets of conventional warfare. In a connected world where people are surrounded by network-accessible devices in their daily lives, attackers now have access to a whole host of new targets. Now, organizations keep all of their business data in network-attached data stores. Militaries control their weapons via networks and rely on poorly protected electronic systems for communications and other uses. Intelligence agencies and corporate intelligence specialists spy on other countries, corporations, and their own citizens.

Technological progress has changed the world as you know it. Whereas once people were needed to access data, to control systems, and to gather information, you now live in a world where computers perform each of those tasks. Targets in the information age include cell phones, satellites, laptops, building and home automation systems, and even embedded systems like smart televisions and appliances. These pervasive parts of this computer-based lifestyle can give an attacker access to very targeted intelligence, the ability to shut down or harm critical infrastructure, or the broad media exposure needed to create widespread panic. Previously only within the reach of a national government or large corporation, intelligence-gathering and attack capabilities are now within the grasp of small groups or individuals. Those with the resources to develop broad arrays of cyberattack tools can pick and choose which data they acquire and how.

Unfortunately for civilians, the network and telecommunications infrastructure used for the Internet is shared by the nations and their militaries that are targeted in cyberwar. In traditional warfare, civilian targets are generally expected to receive at least some protection. Cyberwar changes that, not only because of the shared infrastructure of the Internet, but also because cyberwar often ignores the traditional military targets. The greater accessibility of the tools and resources needed to wage cyberwar also means that it is often fought between groups that are not nations. They may not even be organizations that existed in a visible way until they attacked a highly visible target.

This chapter first explores the traditional targets of conventional warfare, their history, and why they are generally accepted as targets. Second, it compares them with their cyberequivalents, emphasizing how cyberwar changes the options available for attacking assets. This includes why those assets are useful targets and how to attack them. Third, it reviews ways in which cyberattacks and information operations expand the potential list of targets for combatants in cyberwar. It compares them with the targets often attacked in asymmetric or guerrilla warfare. The chapter also explores who the combatants are. It explores how other nation-states and civilian or other groups can attack traditional military targets. It also explores how nation-states conduct information operations and wage cyberwar against a wide range of targets through a series of real-life examples.

Chapter 2 Topics

This chapter covers the following topics and concepts:

- What traditional military targets are
- What cyberwarfare targets are
- What targets of information operations are
- Who combatants in cyberwarfare are
- How cyberwar compares with other types of warfare

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Describe typical targets in both traditional warfare and cyberwar
- List common types of warfare
- Explain why cyberwarfare often more directly targets civilian infrastructure
- Describe typical combatants in cyberwar
- Describe methods used by attackers and their similarities and differences from traditional combat

Traditional Military Targets

The basic targets of military strategists and commanders in conventional warfare have not changed significantly for thousands of years. The names and specifics of the units and technologies may have evolved over time from log and stone forts, dirt roads, and men on foot or horseback to pillboxes and underground bunkers, railroads and airplanes, and armored vehicles. But the basic reasons they have been important targets when nations go to war haven't changed. Military action is still conducted against military targets, infrastructure, communications, supply chains, and the research and development systems behind them.

This is because the goal of conventional warfare is to defeat the enemy's military, thus causing the opposing country's surrender, or at least a negotiation of terms between the opposing sides. This type of conventional warfare is often more palatable to both sides in the conflict than an all-out, no-holds-barred war would be because it generally avoids directly targeting civilian populations or the total destruction of a country to win. When the combatants are not as well matched in size or capabilities, or there are deep underlying divisions between them, they may resort to other means than just conventional warfare.

Common Types of Warfare

Descriptions of how conflicts are fought frequently include several types of warfare. As you read this chapter, think about how each of these applies to cyberwarfare. Think about how cyberwarfare and information warfare techniques can change how each of these types of combat is waged. The common types of warfare include:

- **Conventional warfare** is fought with traditional military tactics and weapons. It is what most people think of when they envision war. Conventional warfare is fought against an enemy's military, thus forcing surrender or negotiation. Conventional warfare is often conducted in accordance with international treaties, laws, and agreements that set limits on behaviors related to combat and combat-related activities.
- **Unconventional warfare** tries to change how an enemy feels about the conflict by suggesting that peace cannot be achieved without giving in or compromising. Unconventional warfare is typically waged in the minds of an enemy populace, rather than their military and leaders. At times, more traditional military targets are used, but for psychological effect, rather than to win in combat. This type of attack is called psychological operations (PSYOPS) in U.S. information operations doctrine.
- **Asymmetric warfare** is fought between groups whose military power, tactics, or strategies are very different. As world history has shown, small groups that are not militarily stronger can sometimes defeat, or at least force a stalemate or withdrawal by a larger force. In fact, **guerrilla warfare**, terrorism, and antiterrorism all fit within the description of asymmetric warfare. Many of the conflicts in the modern world can be properly called asymmetric warfare.
- **Total warfare** is fought using all available resources. Traditional rules of war are set aside, and civilian and military targets are considered acceptable.

Conventional warfare between roughly similar **nation-states**—formally recognized countries or nations—is not the only type of warfare. In fact, unconventional warfare and asymmetric warfare have both been increasingly prevalent during the years since World War II. Later in the chapter, you'll examine cyberwarfare in relation to each of these types of conflict. First, though, to better understand cyberwar's place in modern conflict, you need to understand which targets are typically considered acceptable in conventional warfare and why.

Military Targets in Conventional Warfare

The broad variety of legitimate modern military targets in conventional warfare can be broken into a few categories:

- **Military targets**
  - Military forces and other combatants
  - Military leadership
  - Bases and base facilities
  - Fortifications and strong points
  - Supply depots and maintenance facilities
  - Other military installations
- **Infrastructure targets**
  - Communication infrastructure, such as fiber-optic and copper lines, satellites and satellite communications systems, cellular towers, and radio transmitters
  - Transportation infrastructure, including roads, bridges, waterways, railroads, and airports, as well as the vehicles using them
  - Power-generation capabilities primarily supporting military uses
- **Communications targets**
  - Broadcasting and television stations
  - Telephone, network, and telegraph exchanges of fundamental military importance
- **Supply chain targets**
  - Factories that produce military equipment and arms
  - Production, research, and design facilities that are primarily military-related
  - Supporting infrastructure for the supply chain
- **Military research targets**
  - Laboratories
  - Testing grounds
  - Engineering facilities primarily focused on military research and development

Nations have designed strategies around these targets, and battles have been fought over them throughout history for the same reason that modern military tacticians would focus on them: Defeating a nation-state in traditional warfare normally requires defeating its military. That military often cannot be fully defeated without targeting the entire organization behind it. Conventional warfare still relies on a few basic assumptions about the combatants:

1. That the combatants are nation-states, or that they at least have some form of military that can be separated from the civilian populace. In cases where this isn't possible, such as guerrilla warfare, popular revolutions, and other combat that doesn't fit the norm for traditional warfare, this is much more difficult if not impossible. Treaties that define the rules of warfare sometimes treat combatants who are not part of a formal military structure differently for this very reason.

2. That the supporting infrastructure for the combatants can be determined. In the case of a nation-state, it is simple enough to presume that targeting that nation's infrastructure within its national borders is militarily acceptable, or at least may be deemed necessary during warfare. When fighting a guerrilla war, this becomes much more difficult. The supply chain for combatants is often the same as the one supplying noncombatants, and the guerrilla fighters typically blend into the civilian populace.
3. That the combatants intend to follow the commonly accepted rules of warfare, or those set forth in treaties. The commonly accepted targets presume that there is a desire to fight according to the commonly accepted rules of warfare outlined in international treaties like the **Geneva Conventions**. (These are discussed in more depth later in this chapter.) When that is not the case, the rules and accepted behaviors combatants use and expect can be grossly divergent. During wars fought by the United States and other countries in the latter half of the twentieth century and the early part of the twenty-first century, the rules followed by military units have provided a host of such examples. For example, asymmetric combat, such as that fought against insurgencies, guerrilla fighters, and terrorist groups, may be fought with one side following the laws of armed conflict to a greater or lesser degree, and the other fighting without such limitations.

As mentioned earlier, these assumptions have been written into a number of treaties, laws, and directives that define behaviors and targets between signatory countries. They do not apply, however, when combatants are beyond the bounds of those agreements or are willfully violating them.

Acceptable Targets, Treaties, and International Law

Much like many armed conflicts of the modern era, cyberwarfare is often fought between combatants who haven't formally declared war. Or the combatants cannot formally declare war in an internationally recognized way because they are not nation-states with the ability to do so. Combatants frequently include both nation-state military and intelligence technical assets, nationalist and antinationalist groups, and even small groups and individuals spread around the world. With a variety of combatant types and frequently no formal declaration of war, the choice of acceptable behavior ranges from militarily acceptable combat to electronic warfare that is only restricted by the creativity and the technical capabilities of the combatants.

This wide range of scenarios doesn't mean that there aren't limitations in place that could apply to cyberwarfare. International codes of wartime conduct include broad restrictions on targets. These could be interpreted in some cases to apply to digital attacks.

Unlike the rules of traditional warfare, the international community has not agreed to cyberwarfare treaties and accepted practices. Recently, work has begun in the form of a NATO-sponsored document called the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, but no international law is currently in place. For now, the Geneva

A Brief History of 100 Years of the Laws of War

Rules for warfare have existed for thousands of years, with examples appearing in the Bible, the Quran, and, in more recent history, the Declaration of Independence. In the United States, a formal code of wartime conduct has existed since President Abraham Lincoln issued the Lieber Code in 1863. The Lieber Code described how to treat captured populations, types of warfare that were unethical or inhumane, such as the use of poison or torture, how wars were started and ended, and what punishments were appropriate for those who violated the rules of war.

On the international front, the concept and custom of declaring military objectives separate from civilian targets has a long history in modern warfare. The First Hague Convention in 1899 and the Second Hague Convention in 1907 established both widely accepted laws of warfare and those activities that would be considered war crimes. The Hague Conventions formed a basis of behavior in warfare that included prohibitions against attacking undefended towns and using specific technologies like chemical warfare and special bullets designed to do greater damage to human bodies. They also set conventions regarding how countries could formally declare war and how neutral powers were to be treated.

In addition to the Lieber Code and the Hague Conventions, the Geneva Conventions are likely the most recognized twentieth-century international agreements regarding warfare. Like the Hague Conventions, the term *the Geneva Conventions* actually refers to a series of conventions or treaty agreements, starting with the treatment of sick and wounded servicemen and adding various conventions on handling prisoners, noncombatants, and protection of the victims of conflicts.

Over time, the parties to the Geneva Conventions have added further clarifications regarding when they apply—from their original use during conventional, international-declared warfare to the 1949 addition of coverage for police actions and other nontraditional armed conflict.

Conventions and other international treaties on warfare may be the best tools available when formal national military assets are being used. Unfortunately for those in the line of fire, most attacks are not being openly conducted as part of a formal, acknowledged, military operation during conventional war.

FYI

The United States Department of Defense requires compliance with the Geneva Conventions as part of DoD 2311.01E, issued in 2010. The policy requires that DoD component organizations and contractors follow the laws of war regardless of the type or characterization of a conflict. It defines responsibilities for compliance, requires reporting of incidents, and establishes when legal review is required.

NOTE

Although psychological operations are an important part of information operations, the U.S. military and other organizations do not consider PSYOPS to be part of cyberwar. Thus, although this text discusses unconventional warfare targets and psychological warfare, keep in mind that there is a formal distinction between cyberwarfare and the broader list of information operations like PSYOPS.

Cybertargets in Unconventional Warfare

Unconventional warfare targets the hearts and minds of opponents, attempting to defeat them via psychological means, or to bring them to the negotiating table knowing they cannot win. Unconventional warfare techniques have been used for centuries, and while techniques have changed over time, the basic reason for unconventional warfare hasn't. Sun Tzu's *Art of War*, a book that is more than 2,000 years old, includes a reference to unconventional warfare: "One need not destroy one's enemy. One only needs to destroy his willingness to engage."

The Internet has made both mass media and more targeted communications far more accessible to individuals and groups, making unconventional warfare a popular starting place for cyberattacks. Social media creates broad exposure and awareness. In addition, attacks on Web sites can garner a high level of visibility, which is very attractive to attackers.

The impact of social media as a tool in unconventional warfare was demonstrated very visibly in April of 2013. The Syrian Electronic Army (SEA) compromised an Associated Press (AP) Twitter account. The SEA quickly used it to send out a tweet that appeared to be a legitimate AP news item that said, "Breaking: Two Explosions in the White House and Barack Obama is injured." Shortly after the tweet, the Dow Jones Industrial Average (DJIA) dropped by 140 points, although it quickly rebounded. The effect on the DJIA is a great demonstration of the power that a single compromised account can wield as part of unconventional warfare.

It isn't just major powers that are targeted for attacks like this, as shown by the 2012 breaches of the Taliban Web site. Attackers replaced the Taliban's propaganda with messages of support for the Afghan government and pictures of executions conducted by the Taliban. A constant battle between supporters and detractors of almost any group with an online presence is under way.

NOTE

One method used in attacks is *social engineering*, the practice of using human vulnerabilities as part of psychological operations and to help with technical attacks during cyberwar.

Common targets in unconventional cyberattacks include traditional mass media, social media, blogs, and even traditional means of communication between individuals. Even attacks against the frequently used methods of communications are a useful tool in information operations to create panic, or to deprive a population of knowledge about events.

Targets in Asymmetric Cyberwarfare

Much like the nearly constant state of guerrilla warfare fought in Afghanistan, Iraq, and other countries over the past decade, violent nonstate actors are now starting to shape how electronic warfare is fought. Organizations without a nation-state command structure can spring up almost overnight and can wreak havoc on infrastructure, communications, and other cybertargets.

As the fabric of everyday life becomes more networked, the threats that cyberattacks create make these organizations and individuals far more problematic for defenders. The more advanced your infrastructure is, and the more it relies on networks, telecommunications, and computer control, the more targets are available to potential attackers. Of course, occupying the technological high ground offers advantages too—including greater electronic and cyberwarfare capabilities and more infrastructure to coordinate, host, and manage attacks and defenses.

This can be seen in current combat situations like U.S. operations in Afghanistan against the Taliban, which have leveraged cyberoperations to a significant extent, according to Lt. Gen. Richard P. Mills. In 2012, *USA Today* quoted General Mills as saying, "I was able to get inside [the enemy's] nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."

Total Cyberwarfare

Total cyberwarfare is the worst nightmare of those who defend networks and infrastructure. Unfortunately, the reality is that there are no commonly agreed to limits on cyberwar activities. The only restrictions on attacks are the abilities of the attackers, the skills of defenders, and the attackers' willingness to deal with the consequences of discovery. For years, national governments have been reluctant to admit to their capabilities, but as you will find, attacks like Stuxnet, Flame, and Aurora are beginning to reveal some of the tools major players are able to leverage for attacks.

The military uses of **cyberintelligence**, cyberattacks, and even total cyberwarfare waged to the full extent of attackers' abilities are all a possibility now. Cyberintelligence refers to intelligence activities related to cyberthreats, including identifying and analyzing their existence and capabilities. Keep in mind that the advanced capabilities of today may become the commonly available tools of tomorrow's guerrilla **cyberwarriors**—combatants in cyberwar, whether formally or informally trained. As society's reliance on computerized and network-connected devices grows, the vulnerability to cyberattacks increases.

Cyberwarfare Targets

As mentioned at the beginning of this chapter, cyberwarfare often makes a broader set of targets available to combatants. Three major reasons for this are:

- First, cyberwar is often waged outside of the traditional boundaries of armed conflict. Further, combatants who may not be nation-states often declare and covertly fight cyberwar.
- Second, civilian systems and networks are a significant portion of the available route to military and nonmilitary targets, and are often easier to gain access to.
- Third, cyberwar does not have an existing body of international law limiting its scope as do the treaties that define targets in traditional combat.

This section looks at examples of cyberattacks and electronic attacks against traditional military targets, targets that are exclusively available to cyberattackers, and targets that combine elements of both.

Cyberwarfare Against Traditional Military Targets

Traditional military targets, such as vehicles, bases, and the military supply chain, remain important targets, particularly when nation-states use cyberattacks against opposing forces. In some cases, cyberattacks use completely new modes of attack. In others, traditional warfare techniques are simply updated to use new technologies, leaving attackers and defenders to relearn old lessons in new contexts. The following examples show traditional targets under attack from computer- and signals-based cyberattacks. They also explore new attacks and exploits that are changing how the world thinks about the systems, applications, and devices that are becoming ever-more important parts of people's lives and culture.

Iran Versus U.S. Drones

New military technologies are a particularly interesting target for cyberwarfare, as the constant pace of technological development means that they may not be as secure as their creators want them to be. Complex new systems often have the same types of vulnerabilities as civilian systems, despite their creators' best efforts. In addition, nation-states have far more resources to aim at them than do small groups of hackers and individuals.

One recent example of an attack against a relatively new technology is the Iranian military's 2011 capture of a U.S. drone. Although drones have been shot down or have otherwise ended up in the hands of non-U.S. forces before, in this case the capture may have resulted directly from a cyberattack. Iran captured the drone, a stealthy RQ-170, purportedly by feeding it false Global Positioning System (GPS) signals, as shown in Figure 2-1. When the captured drone was presented to the world on Iranian state-run TV, the lower portion of the drone was blocked from view. Iranian engineers explained in interviews that the difference in elevation between the drone's base and the place where it actually landed was a matter of meters, resulting in damage to the drone's landing gear as it crashed to the ground while attempting to land.

The U.S. military's assessment, including that of analysts at the time, was that Iran did not have the technological sophistication to spoof GPS signals and capture a drone. However, evidence suggests that this might not be the case. Iran has continued to release

FYI

GPS spoofing isn't an unknown or top-secret military technique. University of Texas at Austin Professor Todd Humphreys and his research team have successfully spoofed GPS signals to both drones and an $80 million superyacht, demonstrating the relative ease with which an attack like this can be conducted. You can watch Professor Humphreys' TED talk about how this was done at *http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps*.

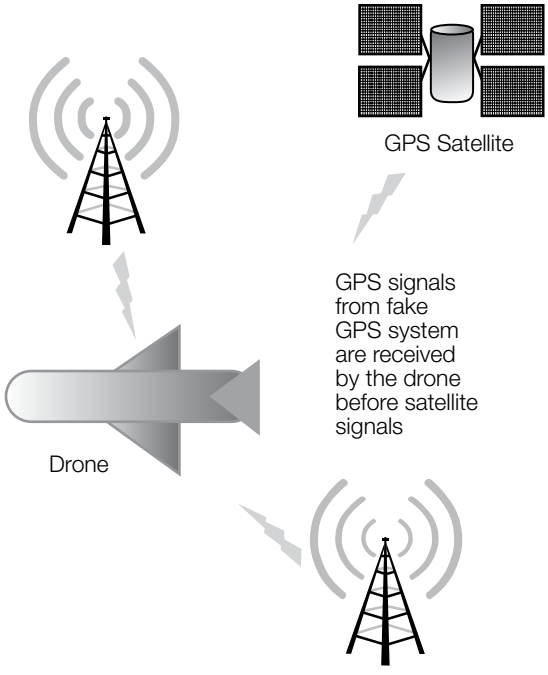

FIGURE 2-1
A theoretical representation of how a GPS-guided drone could be deceived by fake ground stations using a more powerful or closer GPS signal than that provided by GPS satellites in orbit.

data about the drone, including an early 2013 announcement that it had decoded the video stored aboard the RQ-170, which the Iranians then released portions of.

Of course, new technologies aren't the only target for military cyberattacks. Information remains a major target, and malware can be used to replace traditional military intelligence. One of the most important examples of this type of cyberwarfare tool is the Flame malware package, which was discovered infecting systems in Iran, Syria, Sudan, and other Middle Eastern countries (see Figure 2-2).

FIGURE 2-2
The Flame malware's infection focused on Middle Eastern countries, with the highest numbers found in Iran.

Flame: Replacing Spies with Software

In 2012, various computer security organizations announced the discovery of a complex malware package on Iranian and other computers. At the time, it was claimed to be the most complex malware that had ever been seen. The Flame malware appeared to be specifically targeted at Middle Eastern countries, and it had been operating since at least 2010.

As investigations continued, Flame was found to provide a highly modular design, allowing its controllers to add additional components and capabilities. The complex code included advanced compromise techniques, and used a variety of known vulnerabilities to exploit and maintain access to systems. Once on those systems, it could then send information back to controllers, providing a broad intelligence net for the organization that created it.

In 2012, the *Washington Post* claimed that Flame was created by the United States National Security Agency, the Central Intelligence Agency, and the Israeli military in an attempt to gather information prior to cyberattacks against the Iranian nuclear program. Later analysis showed similarities between Flame and the Stuxnet malware that attacked Iranian nuclear facilities in 2010. Both the United States and Israel have denied responsibility.

> **NOTE**
> Complex malware packages with strong infrastructure and support like Flame are called advanced persistent threats.

The First U.S. Cyberwar Strike: Serbia and Kosovo

During the 1999 bombing campaign against Serbia as part of Operation Allied Force, the United States reportedly hacked into the Serbian air defense system. It distorted images the system showed in order to deceive Serbian air traffic controllers. This cyberattack was "essential to the high performance of the air campaign," according to John Arquilla, professor of defense analysis at the U.S. Naval Postgraduate School, in a 2003 PBS interview. This was the first publicized use of offensive information operations by the United States, and is considered by some to be the first known U.S. cyberwarfare operation. An Air Force Office of Information report noted that "The secret new arts of disrupting enemy capabilities through cyber-space attacks appeared to have been a big part of the campaign." However, reports at the time also noted that the full capabilities of the Information Offensive team were not used, and the team was not integrated in ways that would have helped it be fully effective.

Nontraditional Cyberwarfare Targets

In addition to traditional military targets, cyberattacks have been aimed at a variety of nontraditional targets. This section explores political activism and hacktivism, industrial espionage, guerrilla cyberwarfare, and military hacking and cyberattacks against nontraditional targets through a series of examples. As you read these examples, keep in mind the differences between their targets and those that the commonly accepted international laws of war allow.

Political Activism and Hacktivism

Political activism isn't typically thought of as part of traditional warfare, but cyberwarfare has created a new place for activists to make their views visible. It has also made it possible for activist groups to target national governments effectively. Activists are no longer limited to sit-ins, marching with signs, giving passionate speeches, and engaging in strikes. Today, a political activist can shut down his or her target from the comfort of home by attacking a Web site. Or he or she can spread rumors by hacking an official news source and publishing false articles. This online activism is commonly known as **hacktivism**.

> **NOTE**
> Omega, a member of the hacking group the Cult of the Dead Cow, first coined the term *hacktivism* in 1996. Later, Dorothy Denning, a noted cybersecurity and information warfare author, helped to popularize the term in her writings.

In addition to compromising servers, online political activist groups have found ways to make individual, Internet-connected PCs part of effective attack engines. Their politically motivated attacks are often characterized by denial of service (DoS) attacks and attacks against social-media accounts. In addition, online political activist groups bring attention to their chosen issues using social-media awareness campaigns.

Anonymous. Perhaps the most famous currently active online activist group that uses cyberwarfare techniques to target its opponents is the group known as **Anonymous** (see Figure 2-3). Anonymous is a nonstructured group without direct leadership, although strong members of the Anonymous community have led it toward most of its major actions. Because of its lack of internal structure, it is difficult to assign specific motives to Anonymous. However, its members tend to be against Internet censorship, and they often claim to act in favor of human rights, particularly around information and Internet-related freedoms. Somewhat uniquely, Anonymous also tends to have in-person, albeit masked, attendees present as part of its coordinated actions.

Anonymous and Anonymous-related groups have attacked targets associated with a range of issues, from antipiracy efforts, copyright, and digital rights management issues to human rights abuses, child pornography, and hate crime. Their targets have included corporations, government agencies, law enforcement, and others.

Reproduced from Anonymous

FIGURE 2-3
One of the logos commonly used by Anonymous.

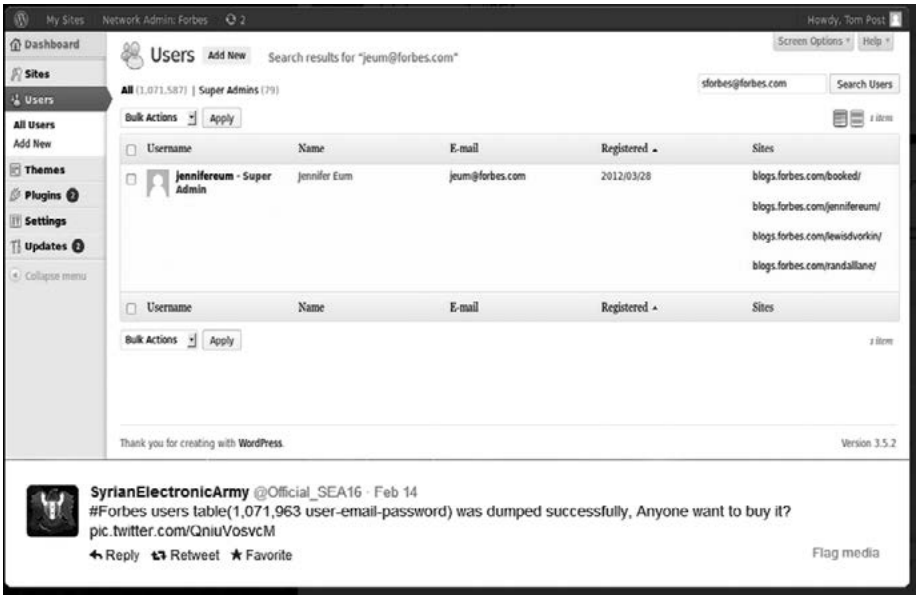

FIGURE 2-4

A screenshot of the Twitter posting of the SEA's successful attack against *Forbes* shows its access to *Forbes*'s internal Web site management console and offers *Forbes*'s user, e-mail, and password database for sale.

Syrian Electronic Army. Some activist groups directly align themselves with a country. The Syrian Electronic Army (SEA) is a group of hackers who support Syrian President Bashar Al-Assad. The SEA targets Web sites belonging to human rights groups and news organizations, among others. Like Anonymous, the SEA also engages in denial of service attacks against organizations that it sees as opposing its political views.

In addition to defacement campaigns and highly visible social-media efforts, the SEA has hacked a number of high-profile organizations. SEA's successful attacks include the compromise of the *Forbes* blog site administrative console shown in Figure 2-4, and a host of defaced Web sites, compromised social-media accounts, and other attacks. For example, the SEA has hacked Harvard University's Web site, breached the popular satire site the Onion's Twitter feed, redirected the U.S. Marine Corps Web site, and hacked the official Facebook and Twitter pages for Skype, among other actions.

Industrial Espionage

Industrial espionage consists of intelligence activities conducted for business purposes, rather than for national security reasons. It is a favorite technique of companies and nation-states looking for information outside their borders. Espionage activities against foreign countries targeted at stealing technologies, research, or information are nothing new in warfare. But the ever-increasing role of computers and electronic communications provides a way to attack companies without resorting to traditional human intelligence and spies.

Aurora: China Versus Google. In 2010, Google released information via the Google blog about a sophisticated 2009 attack against its systems using what came to be called the Aurora (or Hydraq) Trojan. This was a malware application that allowed remote access

to compromised systems. The attack resulted in the theft of source code and other intellectual property from Google, and the attackers attempted to access Google mail accounts of human rights activists. Via its official blog, Google described the attack and noted a few key points:

1. The attack was also aimed at "at least twenty" other major companies in a variety of sectors, including "Internet, finance, technology, media, and chemical" companies.
2. At the time, the attacks appeared to be aimed at "accessing the Gmail accounts of Chinese and Vietnamese human rights activists."
3. Third parties routinely accessed the accounts of dozens of human rights advocates throughout the world. Google suspected this was likely due to phishing scams or malware placed on the individuals' computers.

Although Google never specifically identified where the access occurred, noted security expert Bruce Schneier alleged that the Chinese hackers gained access to a Google-created, backdoor system used to provide wiretap capabilities for Google mail accounts by government agencies.

Over time, further information has come to light suggesting that at least 34 companies were targeted. As of this writing, the security company Symantec had reported that the Aurora attackers are still in operation. Moreover, they appear to have both a large budget and a broad array of unpublished (zero-day) vulnerabilities, which they use to maintain access to compromised systems.

The attack on Google demonstrated the attractiveness of attacks on major cloud communications providers. The presence of a government-required back door for legal compliance meant that attackers had a far easier way to gain access to individual e-mails. It also meant that attackers could use a central tool rather than having to attack dozens or hundreds of individual accounts and passwords.

The sheer number of Google user accounts—and the amount of data that passes through Google and other cloud service providers' data centers on a daily basis—is extensive. This makes Google and other cloud service providers a constant target for attackers seeking the information they possess. Although the civilian communication infrastructure was traditionally a part of intelligence-gathering missions, it is now likely to be directly targeted by military cyberwarfare teams, activists, and other hackers as well.

Saudi Arabian ARAMCO and Shamoon. In August 2012, attackers calling themselves the "Cutting Sword of Justice" targeted Saudi ARAMCO, the most valuable company in the world. They chose Lailat al Qadr, the Night of Power, a major Islamic holy day for the attack. This is a common tactic attackers use to limit the number of defenders who will be on-site or monitoring systems. On the morning of August 15, attackers used a virus to erase data on three-quarters of ARAMCO's corporate PCs, replacing the data with images of a burning American flag. The impact on ARAMCO was significant, resulting in a shutdown of its internal network, e-mail, and Internet access.

FYI

Consider the following interesting facts regarding the possible thought process behind how the Shamoon malware was used:

- The malware was set to take action just as ARAMCO staff left for a one-week vacation, meaning that it had a better chance of going unnoticed for a longer period of time.
- Shamoon only attacked business systems, not those used for oil production. In fact, it had no impact on ARAMCO's oil production.

Thus, although this attack was very visible, it did not directly impact the actual core infrastructure of ARAMCO's oil production. The reasons why an attacker might choose to limit targets in this way might offer insight into the identity of the attackers.

Analysis of the virus showed that it had been built to do two things: destroy data and replace it with the burning flag, and to report back. Analysts named the malware Shamoon after a word found in its code, and found clues to its origin and capabilities embedded within it. The portion of the code that had been used to destroy data was called Wiper, the same name as that of the Flame virus that had targeted Iranian oil companies earlier in 2012.

Although no direct line was found to link Iran to the attack, many analysts believe that the evidence suggests that Iran was responsible for both Shamoon and a similar attack against RasGas, a natural gas company in Qatar.

Industrial espionage attacks can disrupt industry, acquire data to create a competitive advantage, or transfer military or civilian technology. The frequently porous nature of corporate networks presents a relatively low barrier against attack. And such attacks can have an effect out of proportion to the ease with which attackers can implement them. As Shamoon showed, one piece of malware deployed into a corporate network can have a huge impact. If Shamoon had successfully targeted the control systems for ARAMCO's oil drilling, pumping, and other infrastructure facilities, it could have resulted in deaths and destruction of property instead of screens full of nationalist images.

Military Cyberattacks on Nontraditional Targets

As state-sponsored cyberwarfare capabilities grow, their usage against nontraditional targets becomes more likely. Cyberattacks are an increasingly attractive alternative to traditional conflict. Cyberattacks can provide the ability to neutralize an opponent's infrastructure, communications, or other capabilities before, or even instead of, a traditional attack. Because no international law prevents such attacks, they even fall into a gray area if and when they are discovered.

Often, both the attacker and the target keep quiet about nation-states' offensive cyberattacks against nontraditional targets. However, one example was brought to light in 2009, which can help you understand how cyberattacks were seen then and what thought might go into an attack now. This example occurred prior to the invasion of Iraq in 2003.

United States Versus Iraq, a Canceled Attack. According to a 2009 *New York Times* article by John Markoff and Thom Shanker, the United States had prepared a plan prior to the U.S. invasion of Iraq that was intended to "freeze billions of dollars in the bank accounts of Saddam Hussein and to cripple his government's financial system." Worries about collateral damage in the form of financial chaos in the Middle East caused the cancellation of the plan, despite assurances that it would work. Interestingly, the United States did use traditional banking means to freeze Iraqi assets.

Markoff and Shanker point out that the United States targeted Iraq's communications infrastructure using jamming and cyberattacks, and this had unexpected side effects. The attacks "temporarily disrupted telephone service in countries around Iraq that shared its cellphone and satellite telephone systems." This type of attack against communications is far more typical during warfare than disrupting Iraq's financial system via cyberwarfare would have been.

Targets of Information Operations

The targets discussed in this chapter can also be related to the seven major categories of information operations listed in Table 2-1. Remember that the U.S. military's formal definition of cyberwar includes computer network attack, computer network defense, and intelligence gathering. Other information operations categories are not considered cyberwarfare.

TABLE 2-1 Mapping information operations to common cyberwar targets.

INFORMATION OPERATIONS TECHNIQUE	TARGETS
Computer network attack	Networks, computers, and technology systems
Computer network defense	Inbound attacks, malware, and attackers
Intelligence gathering	Stored data, communications, sensor, and other live information
Electronic warfare	Broadcasting capabilities, control channels, GPS signals
Psychological operations	Social media, Web sites, e-mail, and other communications that influence targets
Operations security	Attempts to access friendly information

As you can see, both traditional and nontraditional targets are part of information operations. Attacks can themselves be targets of other attacks, as recovering information about the tool used can provide intelligence about the attacker's identity, capabilities, and goals. In some cases, the tools can even be reverse engineered to use against the original attacker.

Combatants in Cyberwarfare

The variety of possible combatants in cyberwar is as broad as the types of cyberwarfare. Military units with network security and cyberwar capabilities, intelligence organizations, businesses, insurrectionist and terrorist organizations, law enforcement, activist groups, and even individuals can all participate in cyberwar-related activities. Their capabilities, motivations, and the rules they operate by vary greatly. Defenders must be prepared to deal with attackers who have significant resources if defenders have valuable data, infrastructure, or access.

In its broadest definition, any aggressor can wage cyberwar against any opponent. To truly be wide-scale conflict, however, cyberwar must typically involve a state-sponsored group and an opponent that it targets, whether it is another nation-state, an alliance, a guerrilla resistance, an insurrection, or a business.

Military Forces

Modern military units focused on cybersecurity and cyberwar have been an acknowledged part of military service since the early 1990s, when the U.S. Air Force used cyberwarfare techniques in Operation Desert Storm. Although Russian, Israeli, French, and Chinese cyberunits are maintained in relative secrecy, at least some U.S. organizations operate in the public eye. Further, the U.S. policy of developing a strong information operations capability that combines electronic warfare with psychological operations, deception, operations security, and electronic warfare is public knowledge.

U.S. Cyber Command

The United States operates the U.S. Cyber Command (USCYBERCOM), a unified command combining elements of the Air Force, Army, Marines, and Navy. It contributes components of the joint command, which includes a number of information- and cyberwarfare-specific units:

- Air Forces Cyber (24th Air Force)
  - The 67th Network Warfare Wing, an organization composed of five squadrons around the world, operates and defends Air Force networks. It also provides training on network attack and exploit methods, including network warfare capabilities.
  - The 688th Cyberspace Wing has more than 1,200 military and civilian personnel, and operates the Air Force Information Operations Center. The 688th has evolved from an organization that performed electronic warfare operations in Desert Storm to its current form, which specializes in command and control warfare (C2W).
- The Fleet Cyber Command (10th Fleet)
  - Naval Network Warfare Command, a composite organization built from previous organizations, provides network defense and operation.
  - Navy Cyber Defense Operations Command is tasked with command, control, communications, computers, collaboration, and intelligence.
- The Marine Corps Cyberspace Command, the Marine cyberwarfare unit, which has approximately 800 dedicated personnel including:
  - The Marine Corps Network Operations Security Center.
  - The Marine Corps Cryptologic Support Battalion.
- The Army Cyber Command (2nd Army)
  - U.S. Army Intelligence and Security Command provides a variety of services, including intelligence and information warfare capabilities.
  - 1st Information Operations Command performs information operations, including cyberspace defense.

This sampling of the USCYBERCOM's elements shows the breadth and diversity of units that the U.S. Cyber Command includes and demonstrates the strategic importance of cyberwar capabilities for the United States. The U.S. military sees cyberwar as both a threat and a significant part of the United States' war-fighting capabilities, and has increasingly used electronic means of attack as a lower-impact capability than traditional warfare activities.

Guerrilla Cyberwarriors and Insurrectionists

One of the biggest challenges in cyberwar can be identifying your opponent. The systems that an attack comes from may simply be compromised and used to hide the attacker's trail. Even if you recover the tools used, clever opponents make sure the clues they leave in their attack tools take investigators down a false trail. This means that it can be next to impossible to prove an attack is nation-state-sponsored as part of its cyberwarfare program—rather than conducted by a guerrilla group, insurrectionists, or patriots attacking from their own country due to a real or perceived slight.

China's Hacking School

Although no official confirmation exists, China is believed to have one of the largest and most capable state-sponsored hacking training groups in the world. The Aurora attacks discussed earlier in this chapter are generally believed (albeit, without direct proof) to be state-sponsored due to the targeting of Chinese political dissidents as well as information that points to the network origins of the attack. This type of attack doesn't serve typical traditional military purposes, but does reflect the cyberintelligence side of cyberwarfare.

In addition to the Aurora attacks, Mandiant, a security company that tracks advanced computer attacks, reported that it believes that one of the most advanced, long-term cyberattacks that it has been able to identify appears to have been conducted by the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department, part of the Chinese military. The attackers' displayed capabilities support the belief that China has a significant capability to train and use cyberwarfare practitioners.

Mandiant's report on APT 1 can be found at *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.*

In some cases, the best way to identify attackers is by following their social-media presence and their interactions with news organizations. Claiming responsibility for attacks isn't a guarantee that the claims are true, but it can help you to understand where and when guerrilla groups have been active.

The options for asymmetric electronic conventional warfare and unconventional warfare that network attacks provide have been repeatedly exposed during the past decade. But unconventional warfare remains the more accessible option for most guerrilla groups. A few examples include the following:

- The Taliban has consistently advocated using Western technology to overcome the West. In 2013, reports came out that the Taliban may have successfully hacked the navigation systems of a German Heron reconnaissance drone, causing it to crash. It isn't a one-sided fight, however, as both pro- and anti-Taliban attacks have occurred—including repeated compromises of the Taliban Web site. In 2011, for example, one successful attack resulted in the Taliban Web site announcing the death of the Taliban's leader. In an additional example, attackers in 2013 sent a false e-mail in the name of the Taliban spokesman, declaring a temporary end to hostilities.
- In many ways, 2013 was the year that Iranian hackers revealed themselves to be a believable cyberwar threat affecting systems across the world. Iranian hackers successfully attacked U.S. energy companies, universities, and financial institutions, as well as foreign energy firms and other groups. It isn't clear if the attackers were state sponsored or not, but because the attacks came from Iranian universities and companies, the Iranian government was blamed. The attacks may have been in retribution for the Stuxnet worm, which disrupted the Iranian nuclear program.

- An ongoing, low-level cyberconflict has existed in a number of former Soviet republics for years, including Ukraine, where attacks by Russian nationalists took down the Ukrainian president's Web site in 2007. At the time of this writing, cyberattacks were ongoing amidst Ukrainian-Russian tensions, and targets included Ukrainian mobile phone services and the networks that support them.

One of the more interesting developments the Internet has enabled is the ability for civilians to attack nation-states without being present in that country. This means that expatriates, activists, and insurrectionists are no longer limited to fundraising and material support from a distance, and they no longer have to travel to the area where the conflict is occurring to contribute to it.

Individuals and Small Groups

One of the biggest differences between cyberwarfare and more traditional types of warfare is the power a single, focused individual—or a small group of individuals—can exert. Although great leaders and tacticians have changed the direction of battles and wars, individual combatants cannot typically defeat an entire nation's military. Cyberwarfare changes that balance of power, with individuals potentially able to significantly disrupt systems or to change the power balance through their own actions. Now an individual can choose to attack a nation-state, conduct his or her own guerrilla warfare, or use targeted attacks to selectively damage organizations, companies, or other groups.

When these solo hackers, cyberwarriors, and activists succeed, it is typically because they are persistent, highly motivated, and highly skilled. They exploit weaknesses that can be leveraged on a large scale. Sometimes they are motivated by simple curiosity or the desire to prove themselves. But most who can be considered in this context have a purpose beyond that. The following examples look at the effects of individual cyberwarriors, which far outweigh the normal reach of a single person.

The Jester

Individuals aren't always working against a national government. In some cases, they might even be described as patriotic, such as in the case of Th3j35ter (The Jester), an American hacker who targeted the hacktivist group Anonymous mentioned earlier in this chapter.

> "A small team of A players can run circles round a giant team of B and C players" (Th3j35ter, 2010).

Over time, the Jester targeted a series of more than 200 groups ranging from Anonymous to Wikileaks to the Westboro Baptist Church (an American church known for extreme ideologies). He claimed that the Internet provided terrorists with a place to operate safely, and his goal was to prevent that.

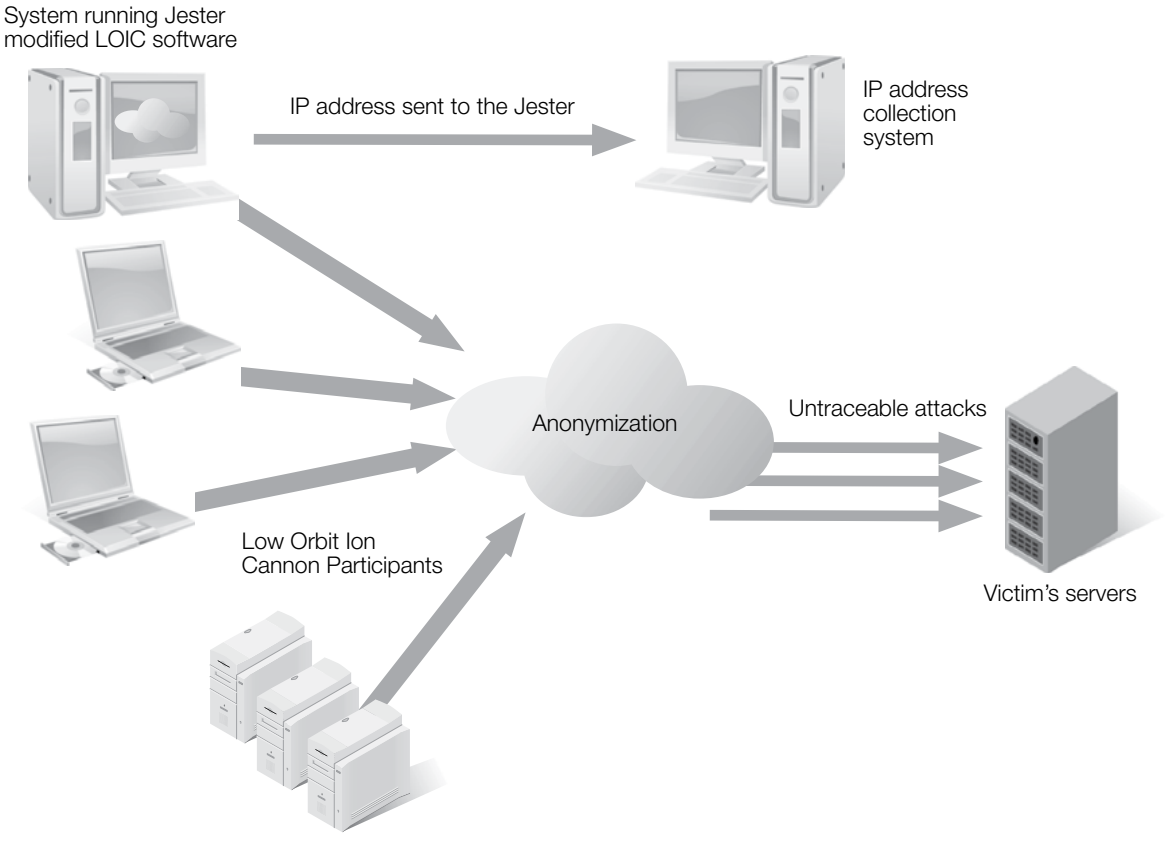

FIGURE 2-5

The Jester's method of defeating the Low Orbit Ion Cannon attack software's anonymization abilities replaced the original software with a version that sent its network address, exposing the system.

The Jester has also engaged in psychological operations. He aimed an attack at one of the most common weapons Anonymous uses, a tool called the Low Orbit Ion Cannon (LOIC). This is a **distributed denial of service (DDoS)** application that provided politically motivated Internet users with an anonymous way to use their computers to support Anonymous. In essence, the LOIC was an Internet cannon that fired traffic from hundreds or thousands of systems at its chosen targets. The Jester claimed that he would remove any chance of anonymity by providing a version that intentionally sent out the actual address of the attacker, thus exposing members of Anonymous (see Figure 2-5).

The Jester has continued to be quite active over time, with other attacks including fake news articles, denial of service attacks against Web sites, and successful campaigns to expose the leaders of hacktivist and hacker groups. He remains active on social media, but has not been publicly identified, despite threats to do so in the past, which led to him create new social-media accounts.

Comparing Traditional Warfare, Guerrilla Warfare, and Cyberwarfare

This chapter has explored the targets that are accepted both in international treaties and traditional wartime behaviors. It has also delved into how cyberwar targets differ from traditional targets and the ways that non-nation-state actors can participate in cyberwar. With a firm understanding of what traditional warfare and cyberwarfare can entail, it helps to add a third type of combat into the mix: police actions, guerrilla, and asymmetric warfare (which this text calls *guerrilla warfare* for convenience). Note that this oversimplifies the concepts each of those descriptions can include, but for the purposes of this text, it is a useful shorthand.

Modern combat often involves groups that are not nation-states, and the ways in which guerrilla warfare is waged are often much closer to how cyberwarfare is conducted. Table 2-2 looks at a few of the most common targets and participants in traditional warfare, guerrilla warfare, and cyberwar. Pay particular attention to the similarities between cyberwarfare and asymmetric warfare.

How Cyberattack Differs from Traditional War

This chapter examined how cyberattacks can be compared with traditional warfare, and how combatants in cyberwar line up with those found in conventional war. A few critical differences are important to keep in mind, however. First, consider the different effects current cyberattacks can cause. Second, consider the blurred lines between cyberwar and personally or financially motivated hacking, where the tools can be used for non-cyberwarfare purposes. Third, consider how surprise and deniability factor into cyberwar. As you consider the difference between traditional warfare and cyberwarfare, keep these differences in mind:

- In traditional warfare, conventional attacks can destroy or significantly damage military units, fortifications, and bases. Cyberattacks are generally not currently capable of that level of physical destruction, although you can see how attacks on infrastructure are possible. It is also easy to predict that attacks that seize control of drones and other remote- or computer-controlled conventional weapons could occur in the future. Thus, for now, the capability for physical destruction by cyberwarfare is lower than that of conventional warfare. But it is likely to increase over time.
- Cyberwarfare activities, particularly low-level cyberwarfare activities, are difficult to distinguish from simple electronic attacks. In fact, the sole difference may be the reason the attack occurs, with cyberwarfare being different simply because is it not conducted for personal or monetary gain.
- Internal political activism doesn't fit with traditional warfare, or even typical asymmetric warfare techniques. However, the tools used by political activists to take down or deface political party Web sites and attempt to change the results of elections are the same tools some actors use in cyberwar.

TABLE 2-2 Comparison of traditional warfare, asymmetric warfare, and cyberwarfare.

	TRADITIONAL WARFARE	POLICE ACTIONS, GUERRILLA, AND ASYMMETRIC WARFARE	CYBERWARFARE
Combatants	Military personnel Intelligence operatives	Military personnel Intelligence operatives Nonstate actors	Military personnel Intelligence operatives Nonstate actors Small groups or individuals
Leaders	National leaders, governments, or military officers	Frequently cell-based, distributed leadership, often with a formal command structure	Sometimes centrally coordinated, such as organized crime or nation-state groups, but also often led by a group, or composed of loosely affiliated individuals
Military targets	Bases, vehicles, weapons, infrastructure Typically avoid nonmilitary-focused civilian infrastructure	Vary from military to civilian	Network-connected or using electronic signals like GPS or Bluetooth
Civilian targets	Civilian infrastructure typically considered a limited target	Civilian infrastructure often considered a legitimate target	Target-rich environment, with many different organizations with differing levels of cyber-security and capabilities
Civilians	Typically considered a limited target	Often considered a legitimate target	Often a primary target, including systems, networks, and infrastructure
Information warfare	Propaganda targeted at opposing forces and civilian populace	Thematic information campaigns against nation-state or other organizations	Disinformation campaigns, Web site, Twitter, and other media platform hacks and account compromises

In addition to these differences, cyberwarfare offers both a new way to use the element of surprise and the chance to disguise attacks, providing deniability.

The Element of Surprise

One of the most effective strategies employed in modern cyberwarfare is technological surprise. Nation-states, commercial organizations, and many other groups build profiles of their expected attackers to assess the risks they face and to plan their defensive strategies. Without detailed information about their opponents' capabilities, however, their guesses are sometimes wrong. That can lead to surprises. The relatively significant impact of Iranian attacks against U.S. and international businesses in 2013 is an example of surprise in cyberwarfare. Traditionally, the United States, Russia, China, Israel, and France have been seen as the only countries with truly viable cyberwarfare capabilities. Iran's entry into the world of cyberwar was a surprise to many, and was more effective because its true capabilities were not known. It is fair to expect that nations with existing cyberwarfare capabilities will continue to be surprised as new opponents bring their capabilities online.

Deniability

Perhaps one of the most interesting differences between cyberwarfare activities and traditional warfare is the ease of deniability for most attacks. It is reasonably easy to cause attacks to come from systems in a country or location that is either a believable attacker or that makes the location of the true attacker very difficult to identify.

Significant attacks like Aurora, Flame, and Stuxnet, allegedly sponsored by nation-states, have been put through in-depth analysis by experts in programming techniques, language, and even analysis of how different cultures tend to craft computer programs. Although that level of analysis can help identify which countries might have created the tool, it is exceedingly difficult to prove that a country deployed it rather than a rogue element or non-nation-state actor, or that it did so purposely. Because of this, well-crafted cyberattacks provide a strong potential for deniability, which can be much harder to ensure in traditional warfare.

CHAPTER SUMMARY

This chapter compared cyberwarfare activities with those typically seen in conventional, unconventional, asymmetric, and total warfare. You learned that conventional warfare is typically fought between nation-states, and has long-standing rules and restrictions found in international treaties like the Geneva Conventions. Unlike conventional warfare, unconventional and asymmetric warfare are frequently fought outside of those rules by non-nation-state groups .

You learned that in modern cyberwar, targets are as varied as the participants. Without broad international treaties or ethical and legal restrictions, those targets are essentially unrestricted. Nonmilitary targets, industry, civilian infrastructure, and even individual noncombatants are all potential targets in a world where there are no accepted cyberwar rules. Nations, guerrillas, insurrectionists, and even small groups and individuals use cyberwarfare techniques to attack each other and to defend their own systems, networks, and infrastructure.

KEY CONCEPTS AND TERMS

Anonymous
Asymmetric warfare
Conventional warfare
Cyberintelligence
Cyberwarriors
Distributed denial of service (DDoS)
Geneva Conventions
Guerrilla warfare
Hacktivism
Industrial espionage
Nation-states
Total warfare
Unconventional warfare