

Nonstate Actors in Cyberwar

CYBERWAR IS PERHAPS THE MOST COMPLEX DOMAIN of modern warfare. Waging war on land, sea, or air requires a significant commitment of financial, human, and political resources. Building and maintaining a potent military force are generally outside the reach of anyone other than a nation-state or an extremely well-organized and funded group. A very small group, on the other hand, can wage cyberwar on a shoestring budget. Although it is certainly true that a well-funded adversary can wage very complex and organized cyberwar, even an individual can engage in cyberwar actions with the computing equipment already at his or her disposal.

There are a wide variety of nonstate actors who play some role in cyberwarfare. These include nongovernmental organizations, organized crime, corporations, terrorists and activists, and even individuals and the media. Their roles may vary widely. Some may wage cyberwarfare activities on their own initiative, while others may simply play supporting or adversarial roles in cyberwarfare. Each adds to the complexity of the cyber environment, and each plays a role that cyberwarriors must keep in mind as they plan cyber domain activities.

Nonstate actors may become involved in cyberwarfare for a variety of reasons, typically related to the reason the nonstate group was organized in the first place. For example, an activist group seeking to gain territorial recognition for a group of displaced persons might use cyberwarfare activities to draw international attention to its cause. Similarly, a group organized in opposition to a nation's belligerent activity might target those cyberwarfare activities as a focus of its protests.

Individuals may also play roles in cyberwarfare, either as participants or agitators. Individual hackers can wage fairly sophisticated cyberattacks with a bare minimum of hardware and software. Although they might not have the resources of a nation-state or a larger organized nonstate actor, they can still engage in significant cyberwarfare activities. Those seeking to defend themselves against cyberattacks must keep such actors under close watch.

Over the past decade, a number of individuals have risen to particular prominence by acting as whistleblowers, bringing the cyberwarfare activities of governments into the public light. These individuals also can have outsized effects on nations by disclosing confidential activities. These disclosures have two major effects on their victims. First, they may compromise some of the specific cyberwarfare weapons a government uses, allowing other adversaries to tailor their defenses to the threat. Second, they may cause governments great embarrassment as their activities are brought into public view for the first time, prompting a debate on their legality and appropriateness in which the government would rather not engage.

Chapter 8 Topics

This chapter covers the following topics and concepts:

- What types of nonstate actors may participate in cyberwarfare
- What roles a nonstate actor may play in cyberwarfare activities
- What motivates nongovernmental organizations to participate in cyberwarfare
- How organized crime participates in cyberwarfare
- What role corporations play in cyberwarfare
- How terrorists and activists use cyberwarfare activities
- How individuals and the media contribute to the cyber environment

Chapter 8 Goals

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

- Explain how nonstate actors participate in cyberwarfare
- Describe the different types of nonstate actors
- Explain the motivations that nonstate actors have for cyberwarfare participation
- Describe the roles that individuals may play in cyberwarfare
- Understand the influence of the media on those engaging in cyberwarfare

Understanding Nonstate Actors

Many different types of nonstate actors play various roles in modern society. Each is organized, either tightly or loosely, to fulfill a specific purpose. Some of these causes are quite noble, such as eradicating human suffering, while others are more questionable and may include the use of terrorist tactics. In this section, you will learn the basic types of nonstate actors that may be involved in cyberwarfare activities. This first section focuses on the characteristics and nature of the actors; the remainder of the chapter discusses the ways that they may engage in cyberwarfare.

Before beginning a discussion of nonstate actors, you must have a clear understanding of the term. In this text, nonstate actors are defined as any entity other than a nation-state that participates in cyberwarfare in any way. This definition is purposefully broad and is intended to encompass the wide range of participants found in the cyber domain, including both large terrorist networks and individual hackers.

Nongovernmental Organizations

Nongovernmental organizations (NGOs) are perhaps the most varied group of nonstate actors in existence today. They consist of essentially any organization that exists outside of the context of a government or a for-profit corporation. They may be organized for a wide variety of purposes, including humanitarian activity, religious purposes, economic development, diplomatic relations, or even armed intervention. They engage in many different types of activities, depending upon their particular mission.

NGOs receive their funding from many different sources. Although they are not part of a government, they often receive funding from one or more governments. NGOs also often solicit private donations to support their activities, calling upon the philanthropic nature of society and the emotional appeal of their missions to raise funds.

There are millions of NGOs in the world, with estimates placing the number in the United States somewhere around 1.5 million. Very few of these play any role in cyberwarfare whatsoever. But a small minority does participate.

Organized Crime

Organized crime, familiar to many from mobster movies glamorizing gangster activity and famous figures like Al Capone and the Gambino family, continues to exist today. Although the days of Tommy gun-toting and “made men” may be behind us, organized crime still flourishes around the world. The U.S. Department of Justice defines **international organized crime** as “self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence.”

The organizational structure, business ventures, and crimes committed by international organized crime groups vary, but, in a 2008 overview of its strategy to combat organized crime, the Justice Department describes them as sharing some or all of these characteristics:

- “In at least part of their activities, they commit violence or other acts which are likely to intimidate, or make actual or implicit threats to do so;
- “They exploit differences between countries to further their objectives, enriching their organization, expanding its power and/or avoiding detection and apprehension;
- “They attempt to gain influence in government, politics and commerce through corrupt as well as legitimate means;
- “They have economic gain as their primary goal, not only from patently illegal activities but also from investment in legitimate business; and
- “They attempt to insulate both their leadership and membership from detection, sanction and/or prosecution through their organizational structure.”

The activities of these organized crime groups are increasingly sophisticated. They include activities far outside the scope of the traditional image of organized crime. According to the FBI, some of the recent actions of international organized crime groups include:

- Wielding pervasive influence in the energy field
- Cooperating with terrorists and foreign intelligence services
- Smuggling illegal contraband and people into the United States
- Conducting money laundering in both the U.S. and international financial systems
- Using cyberwarfare activities to target both individual victims and infrastructure
- Manipulating security markets and engaging in sophisticated fraud
- Corrupting both foreign and domestic public officials
- Using violence and/or threats of violence to maintain and increase their power base

The activities of organized crime remain sophisticated enough that federal, state, and local governments dedicate significant resources to tracking and prosecuting such groups.

Corporations

Corporations are for-profit businesses that are organized by individuals and officially registered by a government. Corporations are granted specific legal rights and, in fact, are recognized as “persons” under U.S. law. They are owned by shareholders and their activities are controlled by boards of directors who are elected by, and act on behalf of, the shareholders. Privately held corporations may have a very small number of owners, whereas shares in public corporations are sold on the open stock market, available to any buyer.

Terrorists and Activists

Many groups seek to actively effect change in the political arena through activities designed to draw attention to their causes and influence public opinion. They fall into two main categories: **activists** and **terrorists**. Activists seek to use peaceful methods, such as demonstrations, boycotts, political campaigns, and non-violent protests to achieve this goal. Terrorists, on the other hand, use unlawful, violent means to create fear among those they seek to influence.

NOTE

Terrorists and activists may also be classified as nongovernmental organizations. However, due to their unique objectives and similarities, this text treats them as a separate category.

Individuals and the Media

In the realm of cyberwarfare, individuals bear unprecedented power. In all other domains of warfare—land, sea, air, and space—there is very little that an individual actor may do to shift the balance of power. In the cyber domain, however, an individual can wield significant power and have a dramatic impact on the actions and capabilities of nation-states and nonstate actors. You need to look no further than the many stories of both hackers and leakers of classified material discussed throughout this text to understand the changing balance of power.

The media plays important roles in magnifying the effect of individuals in cyberwarfare. First, in the case of leakers, journalists may serve as the conduit used to take sensitive information out of government control and place it in the public eye. This was certainly the case with Edward Snowden, who used *The Guardian* and the *Washington Post* to publicly disclose thousands of classified documents from the U.S. National Security Agency (NSA).

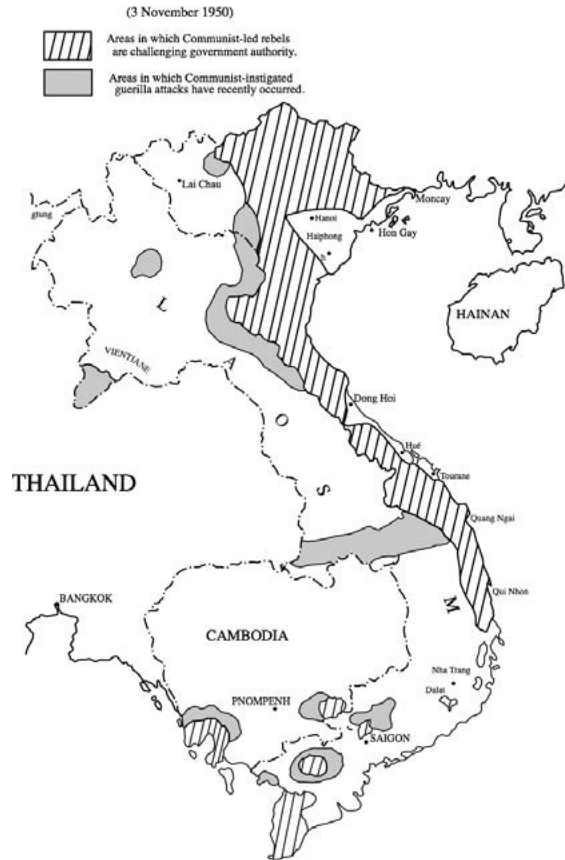
The idea of the U.S. press corps serving as a conduit for disclosing information embarrassing to the U.S. government is not new. A famous historical example of this was in 1971, when the *New York Times*, the *Washington Post*, and others disclosed the **Pentagon Papers**. These documents, leaked by government contractor Daniel Ellsberg, disclosed for the first time that the United States had conducted military operations in neighboring countries during the Vietnam War. Figure 8-1 shows a map from the *Pentagon Papers* documenting CIA activities in Laos, Cambodia, and Vietnam.

The publication of these documents led to a firestorm of public debate that was mirrored in the wake of the Snowden disclosures four decades later. The battle led all the way to the United States Supreme Court, which ruled in June of 1971, in the case of ***New York Times Co. v. United States***, that the papers could continue to be published freely. In his opinion on the matter, Justice Hugo Black stated:

Only a free and unrestrained press can effectively expose deception in government. And paramount among the responsibilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot and shell.

FIGURE 8-1

Map of CIA activities in Southeast Asia first disclosed as part of the *Pentagon Papers* by the *New York Times* in 1971.



Courtesy of NARA

This Supreme Court ruling is often cited in cases where the media leaks classified government materials as part of its reporting efforts.

The media also plays a role in the rise of hackers as individual participants in cyberwar. The exploits of hackers are of significant public interest, and the media reports cases of hacking extensively. John Markoff of the *New York Times* extensively profiled the famous hacker Kevin Mitnick. Some people credit the publicity generated by the *New York Times* and investigation by reporters as contributing to Mitnick's capture. It is certainly true that the media drew Mitnick into the public eye, perhaps encouraging other budding hackers to follow in his footsteps.

The Roles of Nonstate Actors in Cyberwar

How do nonstate actors participate in cyberwarfare? In some cases, these groups may be direct participants, either by serving as the targets of cyberwarfare or by engaging in cyberwarfare activities themselves. Nonstate actors also serve as critics of cyberwarfare activity, exposing acts of cyberwarfare to public scrutiny and/or actively protesting the emergence of cyberwarfare.

Amnesty International Targeted by Cyberattackers

In 2011, American journalist Brian Krebs reported that the nongovernmental organization Amnesty International was the target of repeated cyberattacks. The human rights group's UK Web site was compromised and used to distribute malicious software to site visitors. The software exploited a known vulnerability in the Java programming language to install additional malicious software on site visitors' computers.

Krebs pointed out that Amnesty International had been the target of previous attacks as well—with its Hong Kong-based Web site compromised twice in 2010 and 2011. He speculates that the attackers were probably not trying to gain personal financial information from site visitors. "It appears more likely that the exploit may be part of an ongoing campaign by Chinese hacking groups to extract information from dissident and human rights organizations," Krebs said.

This illustrates the important role that nongovernmental organizations play in the cyber domain. Amnesty International's role in society makes it a natural gathering point for Chinese dissidents and, if this truly was a Chinese-sponsored attack targeted at those dissidents, marks a major exploitation of that group's role for intelligence purposes.

Targets

The rise of nonstate actors in many different types of warfare leads to them becoming targets for cyberwarfare campaigns. The attacks against nonstate actors may be perpetrated by nation-states or by other nonstate actors. Examples of the ways that nonstate actors may be targeted include:

- Web site defacements (such as the Amnesty International attack profiled in the nearby brief, "Amnesty International Targeted by Cyberattackers")
- Surveillance operations against nonstate actors (such as the NSA targeting of Red Cross communications discussed later in this chapter)
- Computer network attacks against computing devices used by nonstate actors

The continued influence of nonstate actors on international relations is likely to lead to a continued focus on them as targets for cyberwarfare activities.

NOTE

The targeting of nonstate actors as the victims of cyberwarfare attack requires that they build and maintain the same types of cyberdefenses businesses and nation-states use. The criticality of cyber-infrastructure to the missions of nonstate actors justifies an investment in adequate defensive technologies.

Participants

In addition to serving as targets for cyberwarfare activities, nonstate actors may also be the aggressors, initiating acts of cyberwarfare against nation-states or other nonstate actors. They conduct these actions to advance their primary goals. For example:

- Terrorists may engage in cyberwarfare to incite fear among the population of a targeted country. For example, a terrorist group may threaten to attack, or actually attack, the power grid in a city or release dangerous levels of water from a hydroelectric dam.
- Organized crime groups engage in cyberwarfare to generate profits for their organizations or incite fear among those they seek to influence in their quest for profits. For example, an organized crime group may use ransomware to extort payments from unwitting victims.
- Activists may engage in cyberwarfare to deface the Web sites of their opponents with political messages sympathetic to their causes. This has two desirable outcomes: spreading their message to the intended audience and embarrassing the legitimate operator of the Web site for having substandard cyberdefenses.

Nonstate actors bring an added complexity to the cyberwarfare world. It is often difficult to determine the sources of their funding and whether they are actually state-sponsored. For example, a recent research report by the security consulting firm Mandiant disclosed the existence of an advanced threat group known as APT1. Although there is no concrete evidence, there is widespread speculation and circumstantial evidence that APT1 is a state-sponsored group funded by the Chinese government. This makes it difficult for an attacked organization to effectively tailor its response. Is it legitimate to target the Chinese government in response to an attack waged by APT1?

Critics

Nonstate actors may also emerge as vocal critics of cyberwarfare activities. The Snowden case illustrated this, prompting a large number of activist organizations to publicly speak out against the U.S. government's surveillance activities.

For example, the American Civil Liberties Union (ACLU), a powerful civil rights lobbying group, strongly opposed the NSA's activities and filed numerous lawsuits objecting to them in court. This activism increased the public scrutiny of NSA activities and presented a legal challenge that the government must respond to in court. In a blog post published several months after the Snowden leaks, the ACLU summarized its position:

When the government operates in secret, it is hard to know anything with confidence. There is, however, one thing you can say with 100 [percent] confidence: we need to know more.

The organization wants to know what information the government is collecting about Americans, what judicial rulings have authorized this collection, and what the government is doing with the information.

The role of the critic in cyberwarfare is to bring to light those activities that may not survive public scrutiny. This is especially effective in democratic governments, where the voice of the people has substantial influence. Critics draw public attention to issues, forcing politicians to take active positions supporting or opposing controversial activities. They also, as in the case of the ACLU, may file lawsuits directly challenging the constitutionality of government activities.

Nongovernmental Organizations in Cyberwar

In the preceding sections of this chapter, you learned about the types of nongovernmental organizations and how they engage in cyberwarfare. In this section, you will learn about specific examples of the ways that NGOs have found themselves the targets of cyberwarfare activities. From aid groups to diplomatic and religious organizations, many different types of NGOs have found themselves at the receiving end of cyberwarfare attacks.

Aid Groups

Aid groups seem an unlikely target for cyberwarfare activities. After all, their humanitarian missions seem like the type of work that would be inoffensive to all. What type of organization would want to target them with cyberwarfare attacks? Furthermore, would any government or nonstate actor run the risk of public embarrassment if they were seen as the aggressors against organizations with humanitarian missions?

Echelon

The *Cryptome* article alleging that the U.S. government targeted the Red Cross claimed that the Echelon system was used to conduct this surveillance. This system was the subject of disclosures about NSA activities in the media around the turn of the century. The system is believed to consist of collection stations located in Australia, the United States, the United Kingdom, Japan, New Zealand, and Canada.

In its 2001 summary of allegations regarding Echelon, *The Guardian* called it “[a] global network of electronic spy stations that can eavesdrop on telephones, faxes and computers. It can even track bank accounts.” The newspaper said the program stores information on millions of individuals on its computers. It noted that the U.S. government has denied the program’s existence, while the British government has given evasive answers to questions.

Is it realistic to believe that intelligence agencies would actually target an aid group in cyberwarfare activities? In 2000, the *Cryptome* Web site published an article alleging exactly that. The authors published what they claimed were excerpts from an unclassified PowerPoint presentation created by an officer in the U.S. Air Force's 544th Intelligence Group. On one of those slides, titled "Our Changing World," the officer stated that there were "A lot of new fish, in a lot of unfamiliar ponds. They are mobile, diverse, and technology has made them advanced." The slides called out nongovernmental organizations, and specifically the International Committee of the Red Cross, as being in that category and asked the question "Friend or foe?"

Diplomatic Organizations

Diplomatic organizations, such as the United Nations, play an important role in international relations. They serve as forums for nations to come together in a neutral environment to discuss pressing issues. They also allow international cooperation on significant issues of human concern, such as the plight of refugees, the welfare of children, and concern for the environment.

Could the United Nations be the target of cyberwarfare activities? It appears quite certain that it already finds itself at the center of actions in the cyber domain. In 2004, the British Broadcasting Company reported that spies in the United Kingdom had eavesdropped on the conversations of then-U.N. Secretary General Kofi Annan. Clare Short, a U.K. cabinet minister, told the BBC that she had seen direct evidence of this, saying that "Well I know—I've seen transcripts of Kofi Annan's conversations."

Perhaps a larger role for the United Nations might be found in the realm of developing guiding principles for cyberwarfare. The International Telecommunication Union (ITU), a branch of the United Nations, has called on governments to:

- Give their people access to communications
- Protect their people in cyberspace
- Promise not to harbor terrorists or criminals
- Promise not to be the first to launch a cyberattack
- Commit to international cooperation to guarantee peace in cyberspace

It is likely that diplomatic organizations will continue to play an increased role in cyberwarfare. In addition to being potential targets for cyber domain activities, these organizations will likely mediate disputes and otherwise become entangled in cyberwarfare issues.

Religious Organizations

Religious organizations are some of the wealthiest, most politically active, and widely connected institutions in the world today. The Roman Catholic Church, for example, claims more than 1.2 billion members in every country around the world. It is among the oldest and wealthiest institutions in the world, with a net worth that likely reaches into the billions of dollars. An organization of this size and significance makes for an interesting cyberwarfare target.

In 2012 and 2013, the cardinals of the Catholic Church gathered in Rome for a conclave that eventually elected Pope Francis. The Italian magazine *Panorama* alleged in a report that the U.S. government monitored the Church leaders' conversations in the period before Francis's election, classifying intercepted communications into four categories:

- Leadership intentions
- Threats to the financial system
- Foreign policy objectives
- Human rights

Leaders on both sides of the table were quick to dismiss these allegations. The Vatican issued a statement that "We don't know anything about this, and in any case we don't have any concerns about it." A spokesman for the U.S. NSA also denied the allegations, saying, "The National Security Agency does not target the Vatican. Assertions that NSA has targeted the Vatican, published in Italy's *Panorama* magazine, are not true."

Organized Crime

Organized crime, seeking to evolve its tactics to meet the challenges of the information age, also plays an active role in cyber activities. These activities include individual extortion attempts, identity theft rings, and using organized hacking groups to infiltrate computer systems around the world.

One tactic often attributed to organized crime is the use of **ransomware**, malicious computer software that takes over a system, encrypting files with a secret key rendering them inaccessible to the legitimate user until he or she pays a ransom. Figure 8-2 shows an example of a message displayed by ransomware after infecting a system.

Along with the intimidation tactics favored by organized crime, the ransomware often makes embarrassing, and completely unfounded, allegations that the victim was targeted because of involvement in child pornography or other illicit activity. The victim, seeking to avoid publicity and regain access to his or her files, often pays the ransom demand, which usually ranges in the hundreds of dollars. This amount is enough to be significant to the organized crime group, but small enough that the victim is likely to pay it without involving the authorities.

FIGURE 8-2

Screenshot of a ransomware payment demand.



Courtesy of Federal Bureau of Investigation/Internet Crime Complaint Center

The risks associated with organized crime are not limited to attacks against individuals and are not constrained by international borders. The Department of Justice recently had this to say about organized crime cyberspace activities in Romania:

One example of the intersection between organized crime and cybercrime is found in Romania. There, traditional Romanian organized crime figures, previously arrested for crimes such as extortion, drug trafficking and human smuggling, are collaborating with other criminals to bring segments of the young hacker community under their control. They organize these new recruits into cells based on their cyber-crime specialty and they routinely target U.S. businesses and citizens in a variety of fraud schemes.

The adaptation of organized crime to changes in economic activity is well documented throughout history. When the government outlawed alcohol during Prohibition, organized crime stepped in and filled the demand for an illicit product. When energy prices skyrocketed, organized crime found ways to generate a corrupt profit. Now that business is moving to cyberspace, organized crime is adopting the principles of cyberwarfare to continue to generate returns.

Corporations

Corporations are completely entangled in the affairs of nations. They are transnational in nature and often pressure governments around the world to make policy decisions favorable to their business interests. In addition, they conduct activities that they want to remain secret from each other, creating an environment where cyberwarfare is arguably inevitable. There are two major ways that corporations become involved in cyberwarfare: through industrial espionage and through cooperation with various governments' intelligence agencies.

Industrial Espionage

Corporations engage in espionage activities against each other as they seek to advance their own competitive business interests. These activities are known as *industrial espionage*, and they may take place based upon the independent actions of corporations or with government support. The objectives of these activities include stealing product plans, learning about competitive bidding processes, and gaining confidential information.

In a report to Congress on industrial espionage, the Office of the National Counterintelligence Executive warned that “The willingness of US scientists and scholars to engage in academic exchange makes US travelers particularly vulnerable not only to standard electronic monitoring devices—installed in hotel rooms or conference centers—but also to simple approaches by foreigners trained to ask the right questions.”

The Federal Bureau of Investigation cites several examples of known industrial espionage attacks against U.S. business travelers. These include:

- Searching of hotel rooms and belongings while travelers were away from their rooms
- Hotels installing monitoring software to eavesdrop on the Internet activities of guests
- Inspection and theft of laptop computers at airports and security checkpoints
- Hacking cell phones to steal contacts, usernames, passwords, and usage history

In addition to these attacks against travelers, foreign intelligence operatives are known to have engaged in cyberwarfare operations against networked computers operated by corporations. The Operation Aurora attacks disclosed by Google targeted U.S. business interests with cyberattacks originating in China. These attacks were focused on gaining access to confidential information stored on corporate information systems.

Game of Pawns

In a 2014 video, the Federal Bureau of Investigation warned students of the risk posed by foreign intelligence operatives. They specifically described targeting efforts against students studying abroad.

The movie tells the story of an American student who spent a year studying in Shanghai and was recruited by the Chinese government agents in a very gradual manner. They began by offering him payments of several thousand dollars to write innocent-sounding white papers on international relations.

The matter escalated out of hand when they paid him \$40,000 and asked him to apply for a job with the Central Intelligence Agency. The story, based upon real-life events, ends with the arrest of the student by federal agents.

Cooperation with Intelligence Agencies

Corporations may also participate in cyberwarfare activities through their cooperation with intelligence agencies as those entities conduct cyberwarfare. One example of this is a program known as PRISM, which *The Guardian* alleges collected information from Internet companies. In PRISM, the government allegedly gained access to information directly from the servers of many major Internet companies:

- Google
- Facebook
- Yahoo!
- Microsoft
- Apple
- YouTube
- Skype
- America Online (AOL)

The Guardian's report states that the NSA is able to use this system to obtain many sources of information about individual users of the companies' products. This data includes e-mail messages, video/voice chats, videos, photos, stored data, Internet usage activity, social network usage, and more.

Although the companies named in the NSA document denied active participation in PRISM, the reporting around this activity prompted a serious national debate on privacy. In response to public pressure, companies began issuing *transparency reports* that disclose the number of government requests for personal information they received.

Terrorists and Activists

Terrorist and activist groups often turn to cyberwarfare tactics because of their disruptive capability. Groups with relatively small memberships and budgets can wage war on a scale that draws international attention to their activities.

Estonia

In April 2007, the Estonian government moved a war memorial erected by the former Soviet Union. Outraged by a move they deemed offensive, many Russians protested the relocation of the memorial and rioting occurred in Estonian streets.

The more interesting outcome of these riots from a cyberwarfare perspective is that they were accompanied by a series of cyberattacks that appeared to originate from Russia. These attacks were distributed denial of service (DDoS) attacks that flooded servers with traffic, attempting to disrupt legitimate use of the servers. The targets included:

- The president of Estonia
- Parliament
- Government offices
- Political parties
- News organizations
- Financial firms
- Telecommunications firms

In response to the attacks, the Estonian government was forced to dramatically limit communication with the outside world, hoping that cutting off Internet access from foreign addresses would allow the systems to recover and begin serving legitimate domestic requests.

Syrian Electronic Army

The Syrian Electronic Army (SEA) is an activist organization composed of hackers who support the Syrian government. It is unknown whether it is actually state-sponsored or independent in nature. SEA is well known for a series of attacks against popular media outlets where it defaced Web sites, replacing content with anti-American and/or pro-Syrian items. For example, in April 2013, the SEA hijacked the Twitter account of the news program *60 Minutes* and issued the tweet:

Exclusive: Terror is striking the #USA and #Obama is Shamelessly in Bed with Al-Qaeda

In an even more serious Twitter hijacking attack that took place that same month, the SEA used the Associated Press account to tweet:

Breaking: Two Explosions in the White House and Barack Obama is injured

This tweet caused an immediate reaction in the financial markets, with the S&P 500 index falling 1 percent in the course of three minutes before quickly recovering. That dip was equivalent to the loss of \$136 billion in equity.

Anonymous

The loosely organized group known as Anonymous is a collection of activist hackers who orchestrate DDoS attacks against targets they select based upon ideological concerns. Recent targets of Anonymous have included:

Operation Payback

One of the best-known actions undertaken by Anonymous was Operation Payback. In this attack, Anonymous hackers took on organizations associated with antipiracy efforts on the Internet. The attack included a PR campaign, which used materials such as the graphic shown in Figure 8-3.

During the campaign, Anonymous launched denial of service attacks against the Web sites of the Recording Industry Association of America and law firms associated with copyright complaints.

Anonymous later redirected these efforts in support of WikiLeaks founder Julian Assange. When financial organizations stopped processing donation transactions for the WikiLeaks site, Anonymous targeted Visa, MasterCard, PayPal, and other firms they felt were complicit in denying WikiLeaks funds.

FIGURE 8-3

Poster used by Anonymous to protest copyright protection efforts during the Operation Payback campaign.



Courtesy of Anonymous

- The Church of Scientology
- PayPal
- Visa
- Sony
- Government agencies
- Child pornography sites
- Copyright protection agencies

The group often releases statements, in text or video form, explaining its actions and attempting to justify its attacks.

Individuals and the Media

Individuals and the media play important and interrelated roles in cyberwarfare. By acting as hackers or leakers/whistleblowers, individuals can wield outsized power against larger forces. The media can trumpet these actions, bringing attention to individuals and their causes. Recent years have seen many cases where both hackers and whistleblowers have caused massive changes in public perception and government policies.

Individual Motivations

Many of the same motivations that encourage them to take part in other illegal and controversial activities cause individuals to take on large institutions and participate in cyberwarfare. Some of the common motivations of hackers and leakers include:

- **Greed**—Individuals may be motivated purely by financial gain and attempt to steal information or compromise systems they will be able to profit from.
- **Technical challenge**—Many hackers seek to demonstrate their technical proficiency to other hackers and the world at large. They engage in cyberwarfare attacks to demonstrate the possibility of successfully attacking large organizations and to gain “street credibility” within the hacker community.
- **Ego**—Many hackers are motivated by simple ego. They want to show their power and demonstrate to the world that they can wield influence.
- **Ideology**—Activists and leakers are often motivated by ideological concerns, seeking to undermine governments or other institutions they oppose or to call attention to what they perceive as illegal or immoral activities.

The true motivations of any individual engaged in cyberwarfare are often mixed and hard to define. In reality, most individuals have a mixture of motives, some noble and some less so. It is important to understand that there are often simple causes that drive individuals to undertake risky, sophisticated attacks against establishment targets.

Hackers

Hackers are the most common example of individual actors in cyberwarfare. The actions of hackers can often be categorized into three groups, based upon the motivation and authority of the individuals waging the attack:

- *White-hat hackers* conduct their attacks under the official sanction of the organization being attacked. These security professionals use hacking techniques to test the security defenses of organizations and point out opportunities for improvement.
- *Black-hat hackers* conduct attacks without permission and with malicious intent. They may be trying to achieve any of the hacker goals, including financial gain, notoriety, or activist objectives.
- *Gray-hat hackers* conduct attacks without permission but without malicious intent. Although many consider their actions illegal, they usually inform the attacked organization of the security risks they uncover.

Kevin Mitnick is one of the best-known examples of a black-hat hacker. Mitnick conducted a series of computer intrusions in the 1990s and was arrested, convicted, and sentenced to prison for his actions. He has been heavily profiled by the media and has garnered business as a computer security consultant (white-hat hacker) since his release from prison.

NOTE

The distinction between a leaker and whistleblower is a fine one and depends upon the perspective of the person applying the label. Although many civil rights activists have branded Edward Snowden as a hero whistleblower, progovernment activists have just as vociferously dubbed him a traitor to his country.

NOTE

Chelsea Manning previously went by the name Bradley Manning before changing her name and gender identity in 2013.


Leakers and Whistleblowers

The actions of leakers and whistleblowers often cause great embarrassment to government agencies that would prefer to keep their secrets from public view. Throughout history, whistleblowers have come forward to call attention to questionable government actions and have been met with mixed reactions. In recent years, several individuals have come forward with classified documents belonging to the U.S. government and released them to media fanfare:

- Julian Assange is the founder of the WikiLeaks Web site. On that site he disclosed a huge quantity of information from government sources in several nations. He rose to prominence when he used the site to publish the Manning documents.
- Chelsea Manning is a former Army soldier who leaked hundreds of thousands of documents to the WikiLeaks Web site in 2010. Those documents included allegations about the Iraq War that deeply embarrassed the U.S. government. They also included more than 250,000 alleged diplomatic cables containing details of relations between the United States and other nations around the world.

- Edward Snowden is a former defense contractor who released a massive amount of information about alleged operations of the National Security Agency in 2013. Snowden worked with reporters from *The Guardian* and the *Washington Post* to release these materials to the public, prompting an international debate about the propriety of government surveillance operations.


The role of the whistleblower has increased significantly since the time of Daniel Ellsberg and the *Pentagon Papers*. The main reason for this transition is the ease with which technology allows modern whistleblowers to steal large quantities of government documents and release them to the media. It is likely that Assange, Manning, and Snowden are not the last names to go down in history for releasing embarrassing information about clandestine government activities.



CHAPTER SUMMARY

The role of the nonstate actor in cyberwarfare is significant. The nature of cyberwar makes it possible for groups of all sizes, and even individuals, to participate in conflict on an unprecedented scale. The tools of the cyberwarrior are simply a computer and an Internet connection. Cyberattacks may be launched from any location against systems located anywhere on the globe. These attacks can target other nonstate actors or larger nation-states and draw international attention when successful and/or high profile.

Students of cyberwarfare must study the role of the nonstate actor carefully and understand how different types of actors play the roles of participants, targets, and critics of cyberwarfare. Nongovernmental agencies, organized crime, the media, individuals, corporations, and other groups play roles in cyberwarfare to advance their political, ideological, and business agendas.



KEY CONCEPTS AND TERMS

Activists	Nongovernmental organizations (NGOs)
Corporations	<i>Pentagon Papers</i>
International organized crime	Ransomware
<i>New York Times Co. v. United States</i>	Terrorists

