CHAPTER

6

Security in Cyberspace

LEARNING OBJECTIVES

Upon completing this chapter, you will successfully be able to:

- Articulate what is meant by *security* in the context of cybertechnology and differentiate issues in cybersecurity from both *cyberprivacy*-related issues and *cybercrime*-related issues,
- Distinguish among three distinct categories of security affecting cybertechnology: *data* security, *system* security, and *network* security,
- Describe key challenges that *cloud computing* poses for cybersecurity,
- Explain what is meant by the terms *hacking*, *Hacker Ethic*, and *hacktivism*,
- Describe the parameters of *cyberterrorism* and show how it can be distinguished both from hacktivism and information warfare,
- Explain what is meant by *information warfare* and show how it is both similar to and different from cyberterrorism.

In this chapter, we examine a wide range of issues affecting cybersecurity. Among them is the question whether cyber intrusions can ever be justified on ethical grounds? For example, would it ever be morally permissible for governmental organizations in (sovereign) nation states to engage in cyberattacks and computer break-ins? The following scenario, illustrating an alleged intrusion involving three nations, briefly addresses that question.

▶ SCENARIO 6–1: The "Olympic Games" Operation and the Stuxnet Worm

In June 2012, the *New York Times* reported that the United States and Israeli governments had been cooperating on an initiative code-named *Olympic Games*. Originally conceived and developed during the George W. Bush administration, the Olympic Games operation aimed at disrupting Iran's uranium enrichment program and thus damaging that nation's nuclear capability. At the core of this joint operation was a computer worm known as Stuxnet, a "cyberweapon" that targeted "electronic program controllers" developed by Siemens Corporation (in Germany) for industrial controlled computers (ICCs) that were installed in Iran. The Stuxnet worm was allegedly responsible for (i) sending misleading data to computer monitors in Iran and (ii) causing several of that nation's centrifuges—that is, fast-spinning machines that enrich uranium—to spin out of control. The Stuxnet attack was estimated to have destroyed approximately 1,000 of Iran's (then) 6,000 centrifuges.[1]

Was the Olympic Games operation a justified breach of cybersecurity? If it is wrong for ordinary individuals and nongovernmental actors/organizations to break into and disrupt someone's computer system, is it also wrong for sovereign nation states to do this as well? Or,

can exceptions be made in the case of cyberwarfare that would justify such actions? We should point, however, that during the Olympic Games incident, no formal declaration of war existed among the three nations allegedly involved (Iran, Israel, and the United States). So, we might modify our original question slightly by asking instead whether imminent threats regarding the development of nuclear weapons by "rogue" nations could be used to justify cyber intrusions on the part of any "legitimate" sovereign nation(s) affected. For example, one might be inclined to argue that such actions against rogue nations could be justified on consequentialist or utilitarian grounds (i.e., based on the principle of "the greatest good for the greatest number"), examined in Chapter 2.

But if it is permissible for sovereign nations states such as the United States and Israel to engage in cyber intrusions against so-called rogue nations like Iran, simply on consequentialist grounds, we can ask the following question: Why would it not also be permissible for some nonstate actors—for example, members of the computer hacking community—to launch cyberattacks against those nations, if an overall greater good could result from their actions? After all, if our concern is merely with the kinds of desirable consequences that would likely be achieved, couldn't the same utilitarian principles justify cyberattacks from hacker groups or from other kinds of nonstate actors/organizations as well? Furthermore, we could ask whether those same actors/organizations might also be justified in attacking "unofficial states" such as Al Qaeda and Islamic State in Iraq and Syria (ISIS), which are not officially recognized by the international community as legitimate and sovereign states.

In February 2015, a well-known international hacker group, called *Anonymous*, announced its plans to take down ISIS by attacking that organization's social media sites used to spread ISIS propaganda and recruit new members.[2] (We describe the Anonymous hacker group in more detail in Scenario 6–3, where we examine that group's activities and practices in the context of our discussions involving some distinctions between hacktivism and cyberterrorism.) On the one hand, some might be inclined to applaud Anonymous' objectives in the case of ISIS. On the other hand, however, we can ask what the unintended consequences might be if we legitimize such activities by international hacker groups like Anonymous, who do not act officially on the part of any legitimate or recognized nation state(s).

We examine controversies affecting cyberterrorism and information warfare (IW) in detail in Sections 6.5 and 6.6, respectively. The purpose of Scenario 6–1, and our brief discussion here of the controversies it raises, is simply to get us to begin thinking about the kinds of state-sponsored hacking/cyber-intrusion incidents that have become commonplace and how these activities pose some significant challenges for implementing coherent cybersecurity polices at the international level. We begin our analysis of cybersecurity issues by defining some basic concepts and drawing some key distinctions.

6.1 SECURITY IN THE CONTEXT OF CYBERTECHNOLOGY

What, exactly, do we mean by "computer security" and "cybersecurity"? Like privacy, security—especially in the context of computing and cybertechnology—has no universally agreed-upon definition. The expressions computer security and cybersecurity are often associated with issues having to do with the reliability, availability, and safety of computer systems, as well as with the integrity, confidentiality, and protection of data. Epstein (2007) suggests that security concerns affecting computers and cybertechnology can be viewed in terms of three key elements:

- Confidentiality
- Integrity
- Accessibility

In Epstein's scheme, confidentiality has to do with "preventing unauthorized persons from gaining access to unauthorized information," while integrity is about "preventing an attacker from modifying data." And accessibility has to do with "making sure that resources are available for authorized users."[3]

Are any additional elements or criteria useful for understanding cybersecurity? Neumann (2004) notes that, in addition to providing desired confidentiality, integrity, and accessibility, cybersecurity aims at preventing "misuse, accidents, and malfunctions" with respect to computer systems. Neumann also notes, however, that cybersecurity can be a "double-edged sword"; for example, it can be used to protect privacy, but it can also be used to undermine "freedom of access" to information for users.[4]

In defining cybersecurity, it is important to point out that sometimes issues involving security in cyberspace overlap with concerns pertaining to cybercrime; other times, however, they intersect with issues involving privacy. We briefly examine some ways in which security issues intersect and overlap with both kinds of concerns, also noting how security concerns can be distinguished from those of privacy and crime.

6.1.1 Cybersecurity as Related to Cybercrime

How are cybersecurity violations both similar to and different from cybercrime? First, we should note that some cyberethics textbooks link together issues involving cybersecurity and cybercrime by covering them in the same chapter. Consequently, these issues could easily be viewed as subcategories of a single cyberethics category. But while most intentional cybersecurity violations are illegal and often criminal, not every crime in cyberspace involves a breach, or violation, of cybersecurity.

Consider three cyber-related crimes that have no direct implications for cybersecurity: A pedophile can use a computer to solicit sex with young children, a drug dealer can use the Internet to traffic in drugs, and a student can use an electronic device to pirate copyrighted music. Although each of these activities is clearly illegal, it is not clear that any of them necessarily result from insecure computers. Perhaps greater security mechanisms on computer networks could deter crimes and detect criminals in cyberspace, but cyber-assisted crimes involving pedophilia, drug trafficking, and pirating music do not typically result from security flaws in computer system design. There are, then, important distinctions between issues of security and crime involving cybertechnology. We will examine issues pertaining specifically to cybercrime in Chapter 7, while focusing our attention in this chapter on concerns affecting security in cyberspace. Just as cybersecurity issues are sometimes lumped together with cybercrime, security concerns involving cybertechnology can also overlap with worries about personal privacy. We briefly considered some of these security-related privacy concerns in Chapter 5. Now we ask: How are issues pertaining to security in cyberspace different from those involving privacy?

6.1.2 Security and Privacy: Some Similarities and Some Differences

The concepts of privacy and security are not always easy to separate, especially when civil liberties and basic human rights are discussed. In the United States, arguments for a right to privacy that appeal to the Fourth Amendment have often been made on the basis of securing the person (and the person's papers and so forth) from the physical intrusion of searches and seizures. Thompson (2001) believes that many of our claims for a right to privacy can be better understood as claims about a "right to being secure." And Moor (2000) argues that privacy can be understood as an expression of (the value) *security*, which he claims is a "core value."

Although cyber-related issues involving privacy and security can overlap, some important distinctions are nonetheless worth drawing. Privacy concerns affecting cybertechnology often

arise because people fear losing control over personal information that can be accessed by organizations (especially businesses and government agencies), many of whom claim to have some legitimate need for that information in order to make important decisions. Security concerns, on the contrary, can arise because people worry that personal data or proprietary information, or both, could be retrieved and possibly altered by unauthorized individuals and organizations.

Privacy and security concerns can be thought of as two sides of a single coin: People need personal privacy, and they wish to have some control over their personal information, especially with respect to how that information is accessed by others. Making sure that personal information stored in computer databases is secure is important in helping them achieve and maintain their privacy. In this sense, then, the objectives for protecting privacy would seem compatible with, and even complementary to, those of maintaining security. In another sense, however, there appears to be a tension between privacy and security. From the perspective of security, protecting (computer) system resources and proprietary data (residing in those systems) is critical, whereas from the vantage point of privacy, protecting personal information and personal autonomy will have a higher priority.

In analyzing the tension involving privacy vs. security interests, Himma (2007a) has argued that threats to security outweigh comparable threats to the right to privacy. On the contrary, Nissenbaum (2010) and Solove (2011) both offer a more sympathetic appeal to the value of privacy in their analyses of the "trade-offs" between the two competing interests. The following quotation, attributed to Ben Franklin (1706–1790), is sometimes cited by privacy advocates to express their interpretation of what is at stake in the dispute involving security vs. privacy interests: "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety." However, in an era where concerns about cyberterrorism now influence our public policy debate, many people may be more willing to give up aspects of their liberty and privacy for greater security. (We examine some impacts that cyberterrorism has for this debate in Section 6.5.) 6.2.1

In the context of cybersecurity, privacy-related concerns include protecting personal data from unauthorized access, abuse, and alteration and thus reflect values that preserve individual autonomy and individual respect for persons. And while anonymity tools (briefly described in Chapter 5) help protect the privacy of individuals navigating in cyberspace, those tools can also cause serious concerns for security because anonymous behavior makes it difficult to identify security violators. So, in some cases, there is a natural tension between security and privacy, as we have seen; at other times, however, the objectives and goals of privacy and security—for example, with respect to confidentiality and data integrity—are the same.[5]

▶ 6.2 THREE CATEGORIES OF CYBERSECURITY

Security issues involving cybertechnology span a range of concerns having to do with three distinct kinds of vulnerabilities:

I. Unauthorized access to data, which are either resident in or exchanged between computer systems

II. Attacks on system resources (such as computer hardware, operating system software, and application software) by malicious computer programs

III. Attacks on computer networks, including the infrastructure of privately owned networks and the Internet itself[6]

We refer to the first of these three categories of security concerns as "data security." The second category of concerns can be described under the heading "system security," and the third can be understood as "network security."

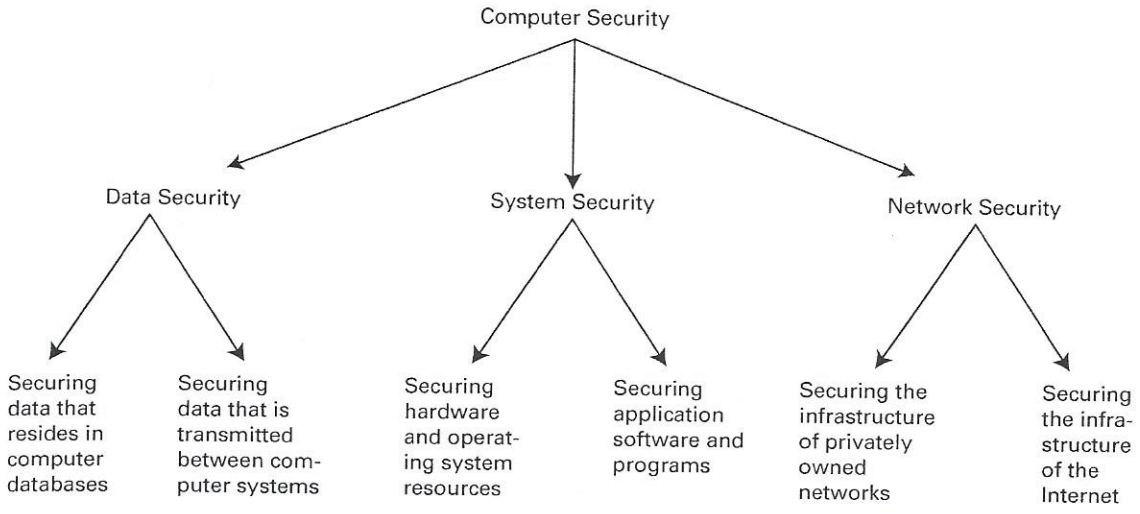

Figure 6-1 Three kinds of computer security.

We briefly describe some key aspects of each category of security, as summarized in Figure 6-1.

6.2.1 Data Security: Confidentiality, Integrity, and Availability of Information

Data security is concerned with vulnerabilities pertaining to unauthorized access to data. Those data can either (i) reside in one or more computer storage devices or (ii) be exchanged between two or more computer systems, or both. In particular, data security issues affect the confidentiality, integrity, and availability of information. Spinello (2000) aptly describes what is required for data security when he points out that

> . . . proprietary or sensitive information under one's custodial care is kept confidential and secure, that information being transmitted is not altered in form or content and cannot be read by unauthorized parties, and that all information being disseminated or otherwise made accessible through Web sites and online data repositories is as accurate and reliable as possible.[7]

Three points in this description are worth highlighting. First, the information to be protected can be either personal or proprietary, or both. (Proprietary information, as we will see in Chapter 8, is legally protected by schemes such as copyrights and patents and thus can be "owned" by corporations or by individuals, while sensitive information is generally considered to be intimate or confidential because it includes personal, medical, and financial records.)

Second, the information must be secured not only from tampering and alteration by unauthorized parties but also from merely being accessed (and read) by those parties. Third, and finally, the stored information must be accurate, readily available, and accessible to authorized parties. So, not only must the information residing in a computer database or in a password-protected Web site be available at optimal times; it must be able to be accessed by authorized users at any time—that is, accessible "on demand."

Data security is now also threatened by "cloud-computing" services (described in Section 6.3), as more and more corporations and ordinary users elect to store their data in "the cloud." Cloud storage devices provide users with one means to secure their data by ensuring that their data could survive (i) "crashes" on the hard drives of their personal computers and (ii) physical damages involving their electronic "tablets" and electronic devices. However, cloud storage also poses a threat to data security because unauthorized users could gain access to, and potentially manipulate, personal and proprietary data that is stored there.

6.2.2 System Security: Viruses, Worms, and Malware

System security is concerned with vulnerabilities to system resources such as computer hardware, operating system software, and application software. As such, it is concerned with various kinds of viruses, worms, and related "malicious programs" that can disrupt and sometimes destroy computer systems. What are the key differences between computer viruses and worms? Dale and Lewis (2016) define a virus as a "malicious, self-replicating program that embeds itself into other code" and a worm as a "malicious stand-alone program that often targets network resources."[8] Worms also differ from viruses because the former do not require human interaction in order to "propagate" in spreading via computer networks (Skoudis 2004). Also, worms can replicate and propagate without needing a host or program (Simpson 2006).

Some security analysts differentiate further between the two types of disruptive programs by pointing out that a worm is less virulent than a virus. However, worms can spread more quickly than viruses, because worms, as noted earlier, do not need any human action to trigger them. Also, worms can move from machine to machine across networks and thus can have parts of themselves "running" on different machines. Viruses, on the contrary, are not capable of running on their own, and they are often activated when an unsuspecting user opens an e-mail attachment.

Some worms and viruses have become well known by their infamous names—not only in the computer community but in the popular media as well. In recent years, prominent viruses and worms have had names such as "Blaster," "Slammer," "Code Red,"[9] "Conficker,"[10] and "Heartbleed."[11] If the distinction between viruses and worms were not confusing enough, some analysts suggest that we further differentiate disruptive programs to include Trojan horses and logic bombs. A Trojan horse often appears to be a benign program, but it can do significant system damage behind the scenes. Logic bombs, on the contrary, check for certain conditions or states in a computer system and then execute when one of those conditions arises. However, many now refer collectively to these various kinds of "malicious programs," including viruses and worms, via the single heading "malware."

Miller (2015) defines malware as "software designed to produce, damage, or provide unauthorized access to computers or computer systems."[12] Employing this broad definition, some forms of "spyware" would also come under the category of malware (i.e., in addition to viruses, worms, Trojan horses, logic bombs, etc.). So, the effects of malware can range from minor annoyances with individual computer systems to preventing an entire organization from operating, to shutting down computer networks, and to disrupting major segments of the Internet.

6.2.3 Network Security: Protecting our Infrastructure

A third category of computer security, which we call network security, is concerned with securing computer networks—that is, from privately owned computer networks such as local area networks (LANs) and wide area networks (WANs)) to the Internet itself—against various kinds of attacks. The Internet's infrastructure has been the victim of several attacks. These attacks have ranged from programs launched by individuals with malicious intentions to individuals who claimed their intentions were benign. In many cases, these attacks have severely disrupted activities on segments of the Internet. In a few cases, they have also rendered the Internet virtually inoperable.

We should note that it is not always easy to determine whether a major computer network disruption is the result of the work of malicious individuals who launch various kinds of malware or is due to the failure of some aspect of the network infrastructure itself. For example, a significant power outage experienced by the AT&T long-distance telephone service in 1990 was attributed to a software glitch in the system's programming code that

caused the network to crash. However, some have questioned the official explanation given by AT&T, suggesting instead that the crash may have resulted from an attack involving malware.

Because many nations now depend on a secure cyberspace for their physical infrastructures, including power grids, there has been increased concern over threats from international hacking groups, including governments and state-sponsored organizations. The following scenario illustrates how vulnerable our national infrastructure may be to attacks by foreign governments.

SCENARIO 6–2: The "GhostNet" Controversy

In 2009, the Information Warfare Monitor (IWM), a Canadian organization that monitors cyberespionage, discovered a network of at least 1,295 compromised computers in 103 countries. Approximately 30% of these were considered "high-value" targets, which (according to the IWM Report) included ministries of foreign affairs, embassies, international organizations, news media, and nongovernmental organizations (NGOs). The computer systems were compromised in ways that suggested China was responsible, but the IWM report refused to identify any one nation. The circumstantial evidence implicating China was tied to the fact that IWM's investigation was launched in response to a request by the Dalai Lama, the exiled leader of Tibet (and longtime enemy of the Chinese government), who reported that his computer network had been hacked. (The IWM report referred to the cyberespionage system as "GhostNet" because it resembled the Ghost RAT (sometimes referred to as Gh0st RAT) Trojan horse malware that was traced back to Hainan, China.) The IWM report concluded that regardless of which country or countries were responsible for the cyberespionage, the discovery of these activities should serve as a warning to policy makers that network security requires serious attention.[13]

In one sense, this scenario might initially seem to be more concerned with information warfare (IW), which we examine in Section 6.6, than with network security. However, the GhostNet controversy has also raised concerns about the vulnerability of a nation's network-based infrastructure, including its power grids. We will return to the GhostNet controversy later in this chapter in our discussion of IW, where we also examine the impact of the Flame virus in 2012.

In this section, we have differentiated three categories of cybersecurity, and we have briefly described some typical kinds of threats associated with each category. Table 6-1 summarizes key concerns identified with each cybersecurity category.

For the most part, the specific cybersecurity issues we identified in this chapter tend to fall into one (or at most two) of these categories. However, in the next section, we will see why some relatively recent security issues associated with "cloud computing" can potentially span all three of the categories comprising our security framework.

TABLE 6-1 Data, System, and Network Security

Cybersecurity Category	Corresponding Area(s) of Concern
Data security	Concerned with vulnerabilities pertaining to unauthorized access to data, as well as with threats to the confidentiality, integrity, and availability of data that resides in computer storage devices or is exchanged between computer systems
System security	Concerned with attacks on system resources (such as computer hardware, operating system software, and application software) by malicious programs
Network security	Concerned with attacks on computer networks, including the infrastructure of privately owned networks as well as the Internet itself

6.3 CLOUD COMPUTING AND SECURITY

What is meant by *cloud computing*? Knorr and Gruman (2008) note that in the past, "the cloud" has often been used as a "metaphor for the Internet." In fact, the graphical interfaces on the screens of older desktop computers typically included an icon or visual of a cloud, which a user could click on to connect to the Internet. But Knorr and Gruman point out that in the current context of "cloud computing," the cloud (in its broad sense) can now refer to any computer resources that are used "outside the firewall."

According to the National Institute of Standards and Technology (NIST; 2011), cloud computing is officially defined as

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services).[14]

Among the "essential characteristics" included in the NIST definition of cloud computing are three key elements: "on-demand self-service," "broad network access," and "resource pooling" (Mell and Grance 2011).

Zeng and Cavoukian (2010) note that while cloud computing is still at an early stage of development, it currently provides a wide range of services—that is, from "full-blown applications to storage services to spam filtering." The authors also believe that cloud computing is changing the way we now think about computing by "decoupling data" and "in effect, divorcing components from location." Consider, for example, that this technology affects not only where users can store their data but also where many of the applications they use can ultimately reside. Four popular examples of cloud-computing applications include photo storing services, such as Google's Picasa; Web-based e-mail services, such as Yahoo; file transfer services, such as YouSendIt; and online computer backup services, such as Mozy.[15]

6.3.1 Deployment and Service/Delivery Models for the Cloud

The NIST definition of cloud computing identifies four distinct "deployment models" and three kinds of "service models," which are also sometimes also referred to as "delivery models" (Zeng and Cavoukian). Deployment models include the following:

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

Whereas (1) is used mainly by "a single organization" that can comprise "multiple consumers (e.g., business units)" and while (2) is used mainly by a "specific community" of organizations and users that have "shared concerns," (3) can be used by the general public. The infrastructure of (4), however, is typically some combination of 1–3 (NIST 2011; Mell and Grance 2011).

As mentioned earlier, cloud computing also provides three important service (or delivery) models:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Zeng and Cavoukian note that while SaaS models deliver various kinds of applications to consumers (i.e., either enterprises or individuals) via a "multitenant architecture," PaaS models deliver "development environments" to consumers. The authors also note that IaaS models

6.3.2 S

TABLE 6-2 Possible Configurations of Cloud Computing

SaaS—Private cloud	PaaS—Private cloud	IaaS—Private cloud
SaaS—Community cloud	PaaS—Community cloud	IaaS—Community cloud
SaaS—Public cloud	PaaS—Public cloud	IaaS—Public cloud
SaaS—Hybrid cloud	SaaS—Hybrid cloud	SaaS—Hybrid cloud

deliver various "resources," which include servers, connections, and "related tools" needed for building "an application from scratch." So if we consider the possible configurations of the cloud-computing services generated by the combination of deployment and service/delivery models, 12 distinct permutations of cloud computing are possible (i.e., based on private/community/public/hybrid modes of deployment and SaaS/PaaS/IaaS modes of service/delivery). Table 6-2 illustrates the permutations.

So it would appear that there is no monolithic scheme for describing and understanding cloud computing in general, given the multifaceted nature of the cloud services currently available. And perhaps more importantly for our purposes, there is no single "context" from which security concerns involving the cloud can be analyzed.[16] Thus, it would seem that any attempt to frame a comprehensive cloud-security policy would need to take into account all 12 elements in Table 6-2. Additionally, it is worth noting that the kinds of challenges involved in securing these elements can impact all three categories of cybersecurity (described in Section 6.2): data security, system security, and network security. In the following section, we focus our analysis on cloud-security concerns that pertain to data/information security, in particular.

6.3.2 Securing User Data Residing in the Cloud

Cavoukian (2008) argues that for cloud computing to be fully realized, users will have to be confident that their personal information is protected and that their data (in general) is both secure and accessible. At present, however, users have at least four kinds of worries along these lines. One concern has to do with how users can control their data stored in the cloud—currently, users have very little "control over or direct knowledge about how their information is transmitted, processed, or stored."[17] Another concern involves the integrity of the data—for example, if the host company goes out of business, what happens to the users' data? A third concern affects access to the data; that is, can the host deny a user access to his/her own data? And a fourth concern has to do with who actually "owns" the data that is stored in the cloud.[18]

Despite these concerns, Cavoukian notes that the cloud offers flexibility and security to users, because they no longer have to worry about how to protect their data. She also notes that the cloud enables users to work on local, less expensive platforms, which could appeal to business owners who would be relieved of the burden of having to secure their data. However, Cavoukian argues that cloud computing can only be effective if users and businesses trust their cloud service providers. But do users have good reasons to place their trust in the businesses that currently provide cloud-computing services? Consider that in 2009, for example, Google reported that a bug in Google Docs (a cloud storage system) had allowed unintended access to some private documents and it was estimated that "0.05% of documents stored via the service were affected by the bug." However, Google claimed that the bug had been fixed within a few days.[19]

According to Talbot (2011), many businesses—especially those in the healthcare and finance sectors—remain leery about turning over their data to third parties. In particular, Talbot identifies three main kinds of concerns that these businesses have: (i) accidental loss of

data, (ii) fear of hacking attacks, and (iii) theft by "rogue employees of cloud providers." So it would seem that until these kinds of concerns are resolved, users have good reasons to be skeptical about placing their trust in cloud-computing services to protect their data. In addition to questions concerning confidence and trust on the part of businesses and ordinary users who subscribe or are considering subscribing to cloud-computing services, some related concerns affecting risk analysis also arise.

6.3.3 Assessing *Risk* in the Cloud and in the Context of Cybersecurity

What is meant by *risk analysis*, and how does it apply in the context of cybersecurity and cloud computing? Schneier (2004), who argues that security is an "ongoing process," believes that a key element in that process involves an understanding of the concept of risk. But who exactly is responsible for understanding risk, as well as for assessing and managing it in computing/information technology (IT) security contexts? Unfortunately, it is not altogether clear where the moral responsibility lies for carrying out these functions. One reason why it is becoming even more difficult to determine who is responsible for doing this may have to do with a factor that Pieters and van Cleeff (2009) call the "deperimeterization" of the security landscape.

Arguing that the information security landscape has become increasingly "de-perimeterized," Pieters and van Cleeff point out that IT systems now "span the boundaries of multiple parties" and they "cross the security perimeters." The authors also note that deperimeterization-related concerns lead to "uncertain risk" for IT security, because of the lack of clear boundaries defining the security landscape. To the extent that there is no secure "digital fence" or perimeter safeguarding the users' data, however, it would seem that ordinary users and businesses alike will be required to assume some level of *uncertain risk* with regard to their data and system resources that reside in the cloud.[20]

So far in Chapter 6, we have examined some key elements in cybersecurity, but we have not yet elaborated on their ethical implications. Next, we examine ethical aspects of cybersecurity that pertain to hacking-related activities.

6.4 HACKING AND "THE HACKER ETHIC"

Individuals who have launched malicious programs of various kinds, which we collectively refer to as malware, have commonly been described in the media as computer hackers. Who are hackers, and what is hacking in the context of computers and cybertechnology? According to Simpson (2006), a hacker is anyone who "accesses a computer system or network without authorization from the owner." (He defines "crackers," on the contrary, as hackers who break into a computer system with "the intention of doing harm or destroying data.") Note that we also examine the concept of hacking in our analysis of cybercrime in Chapter 7, where we focus on hacking as it relates to crime and criminal behavior. In this chapter, we examine hacking and the notion of a "hacker ethic" as it relates to primarily to cybersecurity.

Many in the computer science community are unhappy with how the word "hacker," which now has a negative connotation, is used in the conventional media. Kaufman, Perlman, and Speciner (2002) describe "true computer hackers" in a very different way—that is, as individuals who play with computers for the "pure intellectual challenge" and as "master programmers, incorruptibly honest, unmotivated by money, and careful not to harm anyone." They go on to note that people identified in the media as hackers tend to be malicious individuals who are neither brilliant nor accomplished. The authors also note that "early hackers" have been described as individuals who aimed at accessing computer systems to see how they worked, not to cause any harm to those systems.

In this chapter, we use "hacker" in the sense of the term often attributed to early computer enthusiasts. In documenting early computer hackers, many of whom were associated with the "MIT culture," some authors have used the expressions "hacker ethic" and "hacker code of ethics."

6.4.1 What Is "The Hacker Ethic"?

Levy (2001) suggests that a strong and distinctive code of ethics could be found in the original hacker community. He describes the hacker code as "a philosophy, an ethic, and a dream," based on the following principles:

I. Access to computers should be unlimited and total.

II. All information should be free.

III. Mistrust authority–promote decentralization.

IV. Hackers should be judged by their hacking (not by bogus criteria such as degrees, age, race, or position).

V. You can create art and beauty on a computer.

VI. Computers can change your life for the better.[21]

Perhaps what Levy really describes is not so much a code of ethics but rather a code for the way that hackers approach their craft, that is, in terms of a certain ethic, as in "work ethic." Himanen (2001) has described the hacker ethic as a "new work ethic," which he contrasts with the classic "Protestant work ethic" (coined originally by Max Weber in his classic work *The Protestant Ethic and the Spirit of Capitalism*). In addition to an ethic, hackers also seem to have a distinct "ethos"—that is, they have a distinct way of looking at the world, especially the world of computers.

Many of the early hackers believed that computer systems were inherently flawed and thus needed to be improved. As a result, some hackers believed that they needed total access to all computer systems in order to take them apart, see how they work, and make the needed improvements. Not surprisingly, then, these hackers wanted to remove any barriers to free access to computers. Many hackers have embraced and some continue to embrace, either explicitly or implicitly, the following three principles:

1. Information should be free.
2. Hackers provide society with a useful and important service.
3. Activities in cyberspace are virtual in nature and thus do not harm real people in the real (physical) world.

We briefly examine each principle.

Information Should Be Free

Should information be totally free? If so, on what grounds can this claim be justified? The expression "Information wants to be free" has become a mantra for many hackers who see proprietary software and systems as obstacles to realizing the freedom of the Internet, where users would otherwise have total access to information. The debate over whether information should be free, or even to what extent information should be freely accessible to Internet users, is a complicated one. As we shall see in Chapter 8, this debate is rooted in complex property laws and policies that have been disputed in the courts, often times resulting in Supreme Court decisions. So we will postpone our fuller discussion of this particular point raised by hackers until our analysis of intellectual property in cyberspace. However, a few brief comments need to be made at this point.

Some critics regard the view that (all) information should be free as overly idealistic. According to Spafford (2007), it is also a very naïve view. He points out that if all information were free, privacy would not be possible because individuals could not control how information about them was collected and used. Also, it would not be possible to ensure integrity and accuracy of that information, since information that was freely available could always be modified and changed by anyone who happened to access it. So from the points of view of privacy and confidentiality, a world in which all information was literally and completely free would not be desirable. Thus, there would seem to be good reasons not to embrace the principle that information should be free.

Hackers might object, however, by pointing out that they do not claim that all information should be free because they recognize that some information should be kept private. Hence, they would argue for a position along the following lines: keep private any information that should be private and keep free any information that should be free. They recognize that there is much information that should be kept private but is not, and there is much information that should be publicly available but is not.[22]

Hackers Provide Society with an Important Service

Does the second hacker principle fare any better? Many are suspicious of claims that hackers perform a useful service for society by searching for and exposing security holes in cyberspace. According to this rationale, hackers are doing us a favor, because pointing out these security holes will force those responsible for the holes to fix them.

Spafford has produced a series of counterexamples to this version of the hacker argument, and he uses an analogy to counter the hacker's position that exposing security vulnerabilities is doing the computer user community a favor. Spafford asks whether we would permit someone to start a fire in a crowded shopping mall in order to expose the fact that the mall's sprinkler system was not adequate. Similarly, we could also ask whether you would be willing to thank a burglar who, in the process of burglarizing your house, was able to show that your home security system was inadequate. If you would not, then why, Spafford would ask, should we thank hackers for showing us that our computers are insecure? We return to Spafford's argument in Section 6.4.2. 6.4.2

However, we will see how some nonmalicious hackers have discovered holes in security systems that have also revealed questionable, and possibly illegal, behavior on the part of content providers in cyberspace (as in the case of Sony BMG, which we describe in the next section). So, one might make a utilitarian argument that users are better served if these kinds of abuses are discovered by nonmalicious hackers.

Hacking Causes Only Virtual Harm, Not Real Harm

According to the third principle we identified, unauthorized access in cyberspace causes no real harm because those activities occur only in the virtual world. This argument commits a logical fallacy in that it confuses the relationship between the notions of "harm" and "space" by reasoning that

> the virtual world is not the real (physical) world; so any harms that occur in the virtual world are not real harms.

Consider how this reasoning is flawed. If someone sends you an e-mail message in which they unfairly accuse you of being a malicious person, they have communicated with you in cyberspace, which is "virtual," as opposed to physical, space. But does it follow that the content of the e-mail is any less real than if it had been printed in a hardcopy letter that had been sent to you in the physical mail? Would any harm you experience because of the e-mail's content be any less real than the harm you would experience from identical information in a letter written on physical paper? James Moor has described a variation of this type of reasoning

involving incidents in virtual contexts as the "virtuality fallacy,"[23] which we briefly examined in Chapter 3. In Chapters 9 and 11, we will see how harms involving virtual child pornography can arguably cause real harms to real people, even if they involve only virtual (or computer-generated) images or virtual characters.

Of course, nonmalicious hackers could argue that they are not causing any harm, virtual or real. In fact, some might argue that they are helping to reduce the amount of harm that can occur because of their discoveries of abuses of power by content providers on the Internet, including corporations that provide digital media for electronic devices. For example, it was because of hackers that we discovered that Sony BMG was able to monitor the activities of some unsuspecting customers who purchased digital music products.[24] This questionable, and arguably illegal, activity on Sony's part would likely not have been discovered had it not been for hackers. In this sense, the argument that hackers can prevent harm is similar to, and perhaps builds on, the rationale that hackers provide society with an important service, which we examined in the preceding section.

We have now considered some counterexamples for each of the three principles that we identified as key elements in the "hacker code of ethics." And we have considered some ways in which nonmalicious hackers can respond to those counterexamples. In the following section, we consider the question of whether unauthorized access to a computer in the form of an explicit break-in could ever be ethically justified.

6.4.2 Are Computer Break-Ins Ever Ethically Justifiable?

Eugene Spafford believes that in certain extreme cases, breaking into a computer could be the "right thing to do."[25] He also argues, however, that computer break-ins always cause harm, which suggests that they are not ethically justified. How can Spafford defend what some might interpret as a contradictory claim: Sometimes, it could be right to do something that is ethically unjustifiable? Spafford asks us to consider a scenario in which vital medical data that resided in a computer are needed in an emergency to save someone's life. Further, imagine that the authorized users of the computer system cannot be located. In this case, Spafford believes that breaking into that computer system would be the right thing to do. We might assume that Spafford's rationale is based on utilitarian grounds because, arguably, a greater good (or at least a lesser harm) would result from the computer break-in in this situation.

However, Spafford does not appeal to utilitarian or consequentialist principles to defend his position. Instead, he bases his argument on deontological grounds (see the discussion of deontological and nonconsequentialist ethical theories in Chapter 2) because he believes that morality is determined by actions, not results. He correctly notes that we cannot evaluate morality based on consequences or results because we would not "know the full scope of those results," which are based on the "sum total of all future effect." Thus, Spafford believes that we must base our moral decisions primarily on the actions themselves and not on possible results. In this sense, his view is compatible with the ethical theory of Act Deontology, which we analyzed in Chapter 2.

Critics might point out that Spafford has not provided us with a general principle for determining which kinds of break-ins are ethically justifiable. But using the criteria underlying the act-deontology framework, Spafford could respond by noting that each situation where our two or more (*prima facie*) duties conflict would have to be analyzed on a case-by-case basis in order to determine which duty would take precedence in that particular situation. In deliberating over and weighing between the conflicting duties in those situations, Spafford shows why we cannot simply base our decision on absolute duties (as in Kant's version of rule deontology). (You may want to review David Ross's account of act deontology, examined in Chapter 2, to see how it applies to Spafford's argument for justifying a computer break-in a situation such as the one he presents.)

Independent of whether some computer break-ins can be justified on moral grounds is the question whether certain forms of hacking, especially for nonmalicious purposes, ought to be legally permissible (a question we examine in detail in Chapter 7). Another interesting question is whether the expression "ethical hacker" is an oxymoron. We should note that at least one organization believes that there can be "ethical hackers" and they offer a program that certifies individuals to engage in authorized hacking activities for companies who employ them. According to the Certified Ethical Hacker (CEH) Web site, an "ethical hacker" is an employee within an organization who has been authorized by the organization to "probe" and "penetrate" a targeted computer system or network. Interestingly, but perhaps not at all surprisingly, a "certified ethical hacker" often uses the same tools and knowledge as a "malicious hacker."[26]

Of course, few would disapprove of training people—whether or not we choose to call them "ethical hackers"—to thwart the malicious actions carried by individuals that, for better or worse, we have traditionally called hackers. And the official process of certifying such individuals would seem to give them a sense of legitimacy. But these are not the kind of hackers—if we still wish to use that term to describe these individuals—whose activities would seem to raise moral concerns. However, insofar as these certified hackers' activities also allow "preemptive" hacking attacks, we can question the moral and legal status of some of their actions. We take up this particular question in detail in Chapter 7.

Additional questions regarding hacking could include whether we should distinguish between "white hat" and "black hat" hackers and whether we need to distinguish between hacking and "cracking," as some computer security analysts do. We also address these and similar questions in Chapter 7, where we examine legal issues involving hacking in connection with our discussion of cybercrime.

We have not yet considered the various implications that break-ins involving malicious hacker attacks have had for our financial infrastructure, which increasingly depends on available networked computers. Nor have we yet considered some of the threats that certain forms of malicious hacking pose to our national security. In the next two sections, we examine both security-related concerns.

6.5 CYBERTERRORISM

Concerns about the threats posed by cyberterrorism have been on the rise in the United States and around the world. In 2002 the U.S. Congress passed legislation that specifically responded to this new kind of terrorism, and in 2009 U.S. President Barack Obama established a "cybersecurity czar" to address concerns about cyberterrorism. Obama also announced his plans to create and implement a top-level post called "Cybersecurity Coordinator" to oversee "a new comprehensive approach to securing America's digital infrastructure" and to respond to the threat of cyberattacks from Al Qaeda and other terrorist groups.[27]

What, exactly, is cyberterrorism? Dorothy Denning defines it as the "convergence of terrorism and cyberspace."[28] As such, cyberterrorism covers politically motivated hacking operations intended to cause grave harm—that is, resulting in either loss of life or severe economic loss, or both. Denning (2007) also notes that acts of cyberterrorism are typically performed by "nonstate actors" in their goal of intimidating or coercing governments and societies. In some cases, however, it is difficult to separate acts of malicious hacking (e.g., computer break-ins and cybervandalism) from cyberterrorism. As noted in our discussion of network security in Section 6.2.3, it is sometimes even difficult to determine whether a major computer network disruption is due to a system failure (in either the hardware or the software of a networked computer system) or is the result of the work of either malicious hackers or cyberterrorists.[1] Additionally, it is possible that some of these disruptions are caused a third group: *hacktivists*

6.5.1 Cyberterrorism vs. Hacktivism

In the past, several coordinated cyberattacks directed at major e-commerce Web sites, such as Yahoo and eBay, prevented tens of thousands of people from accessing them. These cyber intrusions, called distributed denial-of-service (DDoS) attacks, resulted in severe economic loss for major corporations. Should these DDoS attacks be classified as cyberterrorism? Or are they better understood as a form of hacking by individuals with some particular political agenda or ideology—a kind of behavior that Manion and Goodrum (2004) describe as hacktivism or "electronic political activism"?

Noting that some hackers and political activists expressed their outrage over the ways in which the Internet had become "commodified" by the early twenty-first century, Manion and Goodrum question whether the actions taken by those individuals could be viewed as a new form of "civil disobedience" that integrates the talent of traditional computer hackers with the interests and social consciousness of political activists. The authors also point out that while many hackers continue to be portrayed in the media as vandals, terrorists, and saboteurs, only a few have considered the possibility that at least some of these individuals might be hacktivists. But they also point out that a key factor in making this distinction is to show that political activists are engaging in acts of electronic civil disobedience (ECD).

Is the distinction drawn by Manion and Goodrum plausible? Can acts of hacktivism be justified on grounds of civil disobedience? Himma (2007b) describes the line of reasoning that hacktivists and their supporters use to justify their acts of civil disobedience, via the following kind of argument:

PREMISE 1. Because civil disobedience is justifiable as a protest against injustice, it is permissible to commit digital intrusions as a means of protesting injustice.

PREMISE 2. Insofar as it is permissible to stage a sit-in in a commercial or governmental building to protest, say, laws that violate human rights, it is permissible to intrude on commercial or government networks to protest such laws.

CONCLUSION. Digital intrusions that would otherwise be morally objectionable are morally permissible if they are politically motivated acts of electronic civil disobedience, or hacktivism.[29]

Based on our analysis of arguments in Chapter 3, we see that the form of this argument is valid. But in order to be a sound argument, the premises must also be true (statements or claims); otherwise, the argument will be valid and unsound. Both of the argument's premises are controversial, and they assume that an appropriate analogy can be drawn between civilly disobedient acts in the physical and the electronic realms. But how are we to understand the notion of "electronic civil disobedience"? Manion and Goodrum claim that for an act to qualify as "civilly disobedient," it must satisfy the following conditions:

- No damage done to persons or property
- Nonviolent
- Not for personal profit
- Ethical motivation—the strong conviction that a law is unjust, or unfair, to the extreme detriment of the common good
- Willingness to accept personal responsibility for the outcome of actions[30]

Based on these criteria, Manion and Goodrum believe that a number of nonviolent, politically motivated cyberattacks could qualify as ECD. Denning (2008), however, argues that Manion and Goodrum's analysis of hacktivism suggests that some acts of Web defacement may also be morally justified as ECD insofar as they are "ethically motivated." But she points out that defacing a Web site seems to be incompatible with Manion and Goodrum's first condition for ECD—that is, "no damage." As Denning notes, defacements can "cause information property damage that is analogous to physical property damage," and both forms of damage can "require resources to repair."[31] So she suggests that at least some of the cases that Manion and Goodman count as hacktivism are questionable, given their own criteria.

Based on Denning's analysis of criteria involving ECD and hacktivism, we ask whether the incident described in the following scenario can be justified on hacktivist grounds. 6.5

SCENARIO 6–3: *Anonymous* and the "Operation Payback" Attack

In 2012, a self-described hacktivist group called *Anonymous* launched a series of DDoS attacks against commercial and government Web sites in response to two different incidents. For one thing, the group stated that its attack, called "Operation Payback," was in retaliation against the (U.S.) Department of Justice for taking down Megaupload, a massive file-sharing site. For another, Anonymous stated that it was supporting the coordinated January 18 (2012) online protest against two controversial legislative proposals in the U.S. Congress: Protect Intellectual Property Act (PIPA) and Stop Online Piracy Act (SOPA).

While most of the participants in this online protest, including Wikipedia and Google, used tactics that were nondisruptive, Anonymous launched DDoS attacks against the Web sites of organizations that supported the two congressional bills. The sites attacked included not only those of the Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA) but also the sites for the U.S. Copyright Office and Broadcast Music, Inc. (BMI), which collects fees from businesses that use music. (The online protest involving SOPA and PIPA, as well as controversial aspects of these two legislative proposals that sparked this protest, is described in detail in Chapter 8.)

Can these attacks by Anonymous qualify as hacktivism, or are they yet another instance of cyberterrorism? One could argue that because of the *scale* of these attacks, they border on cyberterrorism; but this, in turn, may cause us to question of whether a meaningful distinction can be drawn between acts of hacktivism and cyberterrorism. Is the sheer scale of the attack paramount, or do we need to take into account other aspects affecting the act—for example, the *motive* behind it or possibly its *consequences*? Recall our brief discussion of Anonymous in the opening section of this chapter, where we described this group's intention to take down ISIS Web sites. Could that incident be justified as hacktivism because of the desirable consequences it would likely have for Western nations (as well as other countries currently targeted and victimized by ISIS)? But if that kind of attack qualifies as hacktivism, why wouldn't Anonymous' "Operation Payback" attack in 2012 (on commercial interests on the Web) also qualify as a kind of hacktivism. Consider that Anonymous' motives for taking down both entities were the same.

Denning (2001) has drawn some interesting distinctions between hacktivism and cyberterrorism. She notes that hacktivism, the convergence of activism and computer hacking, uses hacking techniques against a target Internet site in a way that (i) intends to disrupt normal operations, but (ii) does not intend to cause serious damage. Denning also notes that these disruptions could be caused by "e-mail bombs" and by "low-grade viruses" that can cause minimal disruption but would not result in severe economic damage or loss of life.

Cyberterrorism, as we saw earlier, consists of activities intended to cause great harm, such as loss of life or severe economic damage, or both. For example, a cyberterrorist might attempt to bring down the U.S. stock market or take control of a transportation unit in order to cause trains to crash. Denning believes while these conceptual distinctions can be used to differentiate hacktivism and cyberterrorism, the boundaries can become fuzzy as we progress from the

former to the latter. For example, should an e-mail bomb sent by a hacker who is also a political activist be classified as a form of hacktivism or as an act of cyberterrorism? Many in law enforcement would no doubt argue that rather than trying to understand the ideological beliefs, goals, and objectives of those who engage in malicious forms of hacking, much more effort should be devoted to finding ways to deter and catch these individuals. However, the category distinctions that Denning has drawn can help determine the degree of punishment that these individuals should receive.

6.5.2 Cybertechnology and Terrorist Organizations

A major security concern, especially since September 11, 2001, has been how and when terrorist organizations, such as Al Qaeda and ISIS might use cybertechnology to carry out their objectives. We discovered that the terrorists who carried out the highly coordinated attacks on the Twin Towers of the World Trade Center communicated by e-mail in the days preceding the attack. We also have discovered that many members of Al Qaeda, despite the fact that some operated out of caves in Afghanistan and Pakistan, had fairly sophisticated computer devices. Yet it does not seem that these terrorists have yet taken full advantage of currently available forms of cybertechnology in executing their campaigns. For example, some fear a scenario which terrorists use cybertechnology to gain control of an airplane's onboard computer systems and even block the ability of a pilot to override those controls.

Denning (2007) notes that there is evidence that terrorist groups and "jihadists" are interested in conducting cyberattacks. She also notes that there is evidence to suggest they have at least some capability to carry out such attacks and that they are undergoing online training on how to develop the necessary skills. However, Denning also points out that (as of 2007, at least) there is no evidence to suggest either that the threat of cyberattacks from these terrorist groups is imminent or that they have acquired the knowledge or the skills to conduct "highly damaging attacks against critical infrastructure."[32] However, we do know that some of these groups now have the skills necessary to set up and successfully operate social media sites to spread jihadist propaganda and to recruit internationally. We also know that they have adeptly used the latest digital devices and mobile technologies to coordinate high-profile terrorist attacks, such as the "Charlie Hebdo"-related attacks in Paris in January 2015.

6.6 INFORMATION WARFARE (IW)

In the preceding section, we saw that it is not always easy to differentiate acts of cyberterrorism from those of hacktivism. It can also be difficult to distinguish between acts of cyberterrorism and acts of IW. Denning (1999) defines IW as "operations that target or exploit information media in order to win some objective over an adversary." But certain aspects of cyberterrorism also conform to Denning's definition of IW, so what distinguishes the latter from the former? For our purposes, IW is distinguishable from cyberterrorism in three ways. First, IW can include cyberattacks that send misleading information to an enemy. Second, while IW is disruptive and sometimes destructive, it need not involve loss of life or severe economic loss, even though such results can occur. Third, IW typically involves cyberattacks launched by sovereign nations, or nation states, as opposed to "rogue" political organizations and terrorist groups.

6.6.1 Information Warfare vs. Conventional Warfare

Moor (2004) notes that while information has always played a vital role in warfare, now its importance is overwhelming, because the battlefield is becoming increasingly computerized. In the past, warfare was conducted by physical means: human beings engaged in combat, using

weapons such as guns, tanks, and aircraft. Moor notes that during the first Gulf War, in the early 1990s, we saw for the first time the importance of IT in contemporary warfare strategies. Arguably, the war was won quickly by the multinational coalition because it had advantages in cybertechnology. Destroying the Iraqi communications technologies at the outset put the Iraqi army at a severe disadvantage. Moor points out that in the future, warfare may have more to do with information and cybertechnology than with human beings going into combat.

Some analysts point out that IW, unlike conventional or physical warfare, often tends to be more disruptive than destructive. The "weapons" of IW, consisting of logic bombs, viruses, worms, and DDoS attacks deployable from cyberspace, typically strike at a nation's infrastructure. Although these are not the traditional weapons of warfare, the disruption can be more damaging than physical damage from conventional weapons.

Consider once again the GhostNet controversy (described in Scenario 6-2) and its implications for IW. Recall that a report issued by the IWM (2009) included circumstantial evidence that linked various cyberattacks (associated with GhostNet) to China but also suggested that other countries might be involved as well. For example, in 2009, the government of South Korea accused North Korea of running a cyberwarfare unit that attempted to hack into both United States and South Korean military networks to gather confidential information and to disrupt service. North Korea was also suspected of launching the DDoS attacks that disrupted the Web sites of 27 American and South Korean government agencies as well as commercial Web sites such as the New York Stock Exchange, Nasdaq, and Yahoo's finance section (Sang-Hun and Markoff 2009). Next, we consider an IW incident that allegedly involves two Western nations: the United States and Israel.

Recall our brief discussion of *Operation Olympic Games* and the Stuxnet worm in Scenario 6–1. Does this "operation" qualify as an example of IW (or "cyberwarfare")? Insofar as the Stuxnet worm sent misleading information to the Iranian government and its scientists, it complies with the first aspect of IW we described. And because this worm was disruptive (regarding Iran's nuclear program), as well as destructive (i.e., with respect to its effect on Iran's centrifuges), it complies with the second aspect of IW. Third, the Stuxnet attacks were launched (allegedly, at least) by two nation states. So, Stuxnet complies with all three conditions for IW (described earlier). But as we noted in our early discussion of the Olympic Games incident, no formal declaration of war had been made by any of the three nations allegedly involved.

6.6.2 Potential Consequences for Nations That Engage in IW

Why has the Stuxnet/Operation Olympic Games incident caused so much controversy at the international level? To see why, consider once again some of the concerns that arose in the international community in response to the 2009 IW incidents allegedly involving China (in GhostNet) and South Korea. One question that arose in the aftermath of the Stuxnet attacks was whether the United States and Israeli governments were now guilty of the same kind of questionable behavior attributed to China and North Korea three years earlier. If so, should the U.S. government worry about the possible repercussions that its involvement in "Olympic Games" could have for its standing in the international community, as well as for its credibility involving any future complaints that it might make against other nations, especially China? Sanger (2012) suggests that the United States did not think through the international implica-

[illegible] of cyberwarfare in the Olympic Games operations (just as he believes that it

this vulnerability when it warned American businesses—immediately following the media's announcement of the effects that Stuxnet had in Iran—to prepare for similar attacks by bolstering the security apparatus on their computers.

We should note that the Stuxnet worm, discovered in 2010, is sometimes confused with the Flame virus (also known as "Flamer" and "Skywiper"). Like Stuxnet, this virus also has significant implications for IW. Ladner (2012) points out that the Flame virus, discovered in 2012, is "an espionage tool" that can "eavesdrop on data traffic, take screenshots and record audio and keystrokes." Kamlyuk (2012), a security (malware) expert at the Kaspersky Lab in Russia, describes Flame as the "most powerful computer virus in history." Pointing to some differences between Stuxnet and Flame, Kamlyuk notes that while the former was a "small application developed for a particular target with the specific objective to interact with industrial control systems," the latter is a "universal attacking tool kit used mostly for cyberespionage."

Some security experts, including Kamlyuk, also point to a few things that Flame and Stuxnet have in common, in addition to the widely held view that both pieces of malware were developed by nation states. Lee (2012) points out that there is growing evidence to suggest that the development teams responsible for Stuxnet and Flame worked together, in the early stages, on the code for both malware applications. One way in which the two applications are similar is that both take advantage of a "zero day" type of "vulnerability" in the systems they attack. In most cases, software developers are the first to become aware of vulnerabilities (such as bugs or "holes") in their systems that need to be fixed. But in some cases, these vulnerabilities are initially discovered and exploited by malicious hackers. In this sense, the vulnerability is discovered on the "zeroth day," or a(ny) day preceding the discovery of that software's vulnerability by its developer(s).

We should note that IW-related concerns affecting both the Flame virus and Stuxnet worm are further complicated by the recent development of a new kind of search engine, called Shodan. Not only can Shodan locate and return the URLs for relevant Web sites (as traditional search engines do), but it is also able "to map and capture the specifications of everything from desktop computers to network printers to Web servers" that are connected to the internet (Charette 2012). O'Harrow (2012) points out that between 2010 and 2012, Shodan gathered data on approximately 100 million devices, "recording their exact locations and the software systems that run them." He also notes that during that period, Shodan users had discovered numerous ("uncounted") industrial control computers—that is, the systems that automate power grids and water plants—and that these computers were "linked in, and in some cases they were wide open to exploitation by even moderately talented hackers." As Robert Charette observes, it is not difficult to imagine what "a government intent on doing harm to U.S. infrastructural and business systems could do with that information." So, it would seem that the United States (and other countries as well) may indeed have something to worry about in the aftermath of the IW activities involving Stuxnet and the Olympic Games operation.

In concluding our discussion of IW, we acknowledge that some controversial issues surrounding this topic were not able to be examined. One interesting question concerns whether IW could, in principle, satisfy the conditions traditionally required for a "just war." For example, one requirement is that a distinction between combatants and noncombatants be drawn and respected. Another condition is that attacks typically cannot be preemptive. However, it may not be possible for these and other conventional just-war requirements to be satisfied in the context of IW. So, some conclude that IW can never be justified solely on moral grounds. Unfortunately, however, an examination of the necessary conditions articulated for just-war theory in the context of IW is beyond the scope of this chapter.[33]

In this and the preceding section, we have discussed various security threats, from malicious hacking to hacktivism and from cyberterrorism to information warfare. Table 6-3 summarizes these distinctions.

TABLE 6-3 Hacktivism, Cyberterrorism, and Information Warfare

Hacktivism	The convergence of political activism and computer hacking techniques to engage in a new form of civil disobedience
Cyberterrorism	The convergence of cybertechnology and terrorism for carrying out acts of terror in (or via) cyberspace
Information warfare	Using malware in cyberattacks designed to mislead the enemy and disrupt/damage an opponent's military defense system and its critical infrastructure

6.7 CHAPTER SUMMARY

In this chapter, we examined some ethical implications of a wide range of cybersecurity issues, including the question whether unauthorized computer break-ins can ever be ethically justified. We also described some ways in which some cybersecurity issues overlap with cybercrime, while others overlap with privacy. Additionally, we briefly identified some of the tensions that exist between security and privacy in the context of cybertechnology. We then argued that it is useful to draw distinctions involving data, system, and network security, and we briefly considered some of the challenges that cloud computing provides for cybersecurity. Finally, we drew some distinctions between concepts such as hacking and hacktivism and IW and cyberterrorism.

We also drew some distinctions between the traditional and current meanings of "hacker," in our discussion of the "hacker ethic." In Chapter 7, we will examine some criminal aspects of (malicious) hacking from a legal perspective.

REVIEW QUESTIONS

1. What do we mean by "computer security" or "cybersecurity"?
2. Which three key elements does Richard Epstein include in his description of computer security/cybersecurity?
3. Why does Peter Neumann believe that computer security/cybersecurity can be a "double-edged sword?"
4. How can cybersecurity concerns be differentiated from issues in cybercrime?
5. How are cybersecurity issues similar to and different from privacy issues affecting cybertechnology?
6. What is meant by *data security*?
7. What is *system security*, and how is it similar to and different from *network security*?
8. What is *cloud computing*, and what challenges does it pose for securing one's personal information in cyberspace?
9. Identify the four kinds of *deployment* models and the three types of *service/delivery* models comprising cloud computing.
10. Who are computer hackers, and how has the term "hacker" evolved?
11. What is meant by the expression "hacker code of ethics"?
12. According to Steve Levy, what are the six "principles" of this code?
13. Describe and briefly evaluate the argument used by some hackers who assert that "information wants to be free."
14. Assess the argument that (nonmalicious) hackers can provide society with a valuable service. Is it a plausible argument?
15. Describe the kind of argument that some hackers use to support their claim that hacking causes only virtual harm, not real harm.
16. What exactly is cyberterrorism?
17. What is meant by "hacktivism"? How is it distinguished from traditional computer hacking?
18. Can "hacktivist activities" be justified on the grounds of civil disobedience toward unjust laws?
19. What is meant by "information warfare"?
20. How can information warfare be distinguished from cyberterrorism?

DISCUSSION QUESTIONS

21. Is the expression "ethical hacker" an oxymoron? Do you agree that some individuals should be allowed to be "certified" as hackers to work on behalf of industry or for the interests of other organizations? Do the kinds of activities permitted by certified hackers in the CEH program raise any moral issues? Explain.
22. Revisit the GhostNet controversy described in Scenario 6-2 and the "Olympic Games" incident discussed in Scenario 6-1. What kinds of actions should sovereign nations take against countries that engage in cyberespionage and that launch cyberattacks in the form of various worms, viruses, and DDoS requests? Would such attacks be acceptable between nations that have formally declared war with one another?
23. In Section 6.4.1, we examined some issues surrounding a "hacker code of ethics." We also saw why this code, containing the six principles described by Steven Levy, has been controversial. Is it possible to establish an appropriate set of guidelines for a hacker code of ethics, that is, for nonmalicious hackers, without becoming a moral relativist? You may want to revisit our discussion of moral relativism in Chapter 2 in deciding your answer to this question.
24. Revisit the Olympic Games operation (described in Scenario 6–1). Is it morally, or even legally, permissible for "legitimate" (or sovereign) nation states to conduct cyberwarfare against one another? Would it ever be morally permissible for a nation to solicit the help of an international hacking organization, such as Anonymous, in launching cyberattacks against other sovereign nation states or even against radical organizations such as Al Qaeda or ISIS?

Scenarios for Analysis

1. In our discussion of hacking-related security concerns, we saw how some forms of anonymous behavior in cyberspace can cause harm to others. What course of action would you recommend be taken in the following scenario?

   A very close political race is underway in your state, where two candidates are running for a seat in the U.S. Senate. The weekend before citizens will cast their votes, one candidate decides to defame his/her opponent by using an anonymous remailer service (which strips away the original address of the sender of the e-mail) to send a message of questionable truth to an electronic distribution list of his opponent's supporters. The information included in this e-mail is so defamatory that it may threaten the outcome of the election by influencing many undecided voters, as well as the libeled candidate's regular supporters, to vote against him/her. Does the "injured" candidate in this instance have the right to demand that the identity of the person using the anonymous remailer (whom she suspects is her opponent in this election) be revealed?[34]
2. Recall Eugene Spafford's argument as to why computer break-ins can be justified under extraordinary circumstances. Apply his rationale in the following scenario.

   You determine that you will need to break into a neighbor's car in order to drive a friend, who will otherwise die, to the hospital. You realize that you are morally obligated to save a person's life when it is in your power to do so. But you are also obligated to obey the law, which forbids breaking into someone's motor vehicle. How is the reasoning process that you use to evaluate this scenario similar to or different from the one Spafford used in determining whether it is morally permissible to break into a computer database containing the medical information needed to save someone's life?

ENDNOTES

1. Scenario 6–1 draws from information in the accounts of the Olympic Games operation in Charette (2012) and Nakashima and Warrick (2012). See both works for more details regarding the controversies surrounding the Olympic Games controversy and the Stuxnet worm.
2. See Viebeck (2015). Also see the interview with Anonymous in *France 24*, available at http://www.bing.com/videos/search?q=anonymous+isis+interview+in+france+24&FORM=VIRE7#view=detail&mid=8460F5CF64BDD4CCAD428460F5CF64BDD4CCAD42.
3. Epstein (2007), p. 176. Note that Kizza (2008), who has a similar threefold distinction regarding the key elements of cybersecurity, describes the third element as *availability* rather than *accessibility*.

4. Neumann (2004), pp. 208–09. Here, Neumann also provides more examples of how security can be viewed as a double-edged sword that "cuts both ways."
5. Some of the distinctions I make between privacy and security in Section 6.1.2 draw from and expand upon concepts and frameworks introduced in Tavani (2000).
6. We should note that some authors suggest that two categories—data security and system security—are sufficient to cover the issues that fall under the heading "Cybersecurity." The framework I use in Section 6.2, with three separate categories, draws from some distinctions introduced in Spinello and Tavani (2004) and expanded upon in Tavani (2007).
7. Spinello (2000), p. 158.
8. Dale and Lewis (2016), pp. 655–656.
9. Bottis (2007) points out that Code Red infected approximately 395,000 servers during a 14-hour period in 2000.
10. Lawton (2009) notes that the Conficker worm turned the computers it infected into "a botnet capable of launching mass attacks" and that in a four-day period in January 2009, the number of "individual infections grew from 2.4 to 8.9 million."
11. See, for example, the descriptions of this virus included in Aamoth (2014) and Arrouas (2014).
12. Miller (2015), p. 48.
13. Scenario 6–2 draws from information included in Maidment (2009) and the *Information Warfare Monitor Report* (2009). See also "Tracking GhostNet: Investigating a Cyber Espionage Network" (2009). Available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
14. See the fuller description available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
15. Privacy Rights Clearinghouse (2008). My analysis of cloud computing in Sections 6.3–6.3.2 draws from and expands upon some concepts and distinctions introduced in Grodzinsky and Tavani (2011).
16. See Grodzinsky and Tavani (2011) for a more detailed discussion of this point.
17. Privacy Rights Clearinghouse (2008).
18. *Ibid.*
19. See the account of this incident in Breitbart (2010).
20. For an excellent discussion of "risk assessment" in the context of cybersecurity, see the extended analysis in Schneier (2004); a detailed study of risk methodologies affecting cloud computing is included in Pauley (2012).
21. See Levy (2001) for a full explanation of the six principles identified in this list.
22. I am grateful to Mason Cash for pointing out this distinction to me.
23. Moor described this fallacy in a talk titled "Just Consequentialism and Computing," presented at the 2000–2001 Humanities Lecture Series, Rivier University, Nashua, NH, February 2001.
24. See, for example, the analysis of the "Sony Rootkit" controversy in Russinovich (2005). See also the account of this incident in *Wikipedia*. Available at http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal.
25. Spafford (2007), p. 57.
26. See www.eccouncil.org/ceh.htm. I am grateful to Hien Nguyen for pointing out this Web site to me.
27. See http://edition.cnn.com/2009/POLITICS/05/29/cyber.czar.obama/index.html.
28. Denning (2004), p. 536.
29. Himma (2007b), pp. 73–74. Note that Himma's original text has been transposed into the form of a logical argument (with the author's permission). See also Himma (2008).
30. Manion and Goodrum (2004), p. 528.
31. Denning (2008), p. 421.
32. Denning (2007), p. 136.
33. See, for example, Arquilla (2002), De George (2003), Denning (2008), and Lin, Allhoff, and Rowe (2012) for some excellent discussions of the possibility of "just warfare" in the cyber era.
34. I am grateful to an anonymous reviewer who suggested this hypothetical scenario, illustrating an ethical dilemma involving Internet anonymity.

REFERENCES

Aamoth, Doug. 2014. "How to Protect Yourself Against the Heartbleed Bug." *Time*, April 9. Available at: http://time.com/55337/how-to-protect-yourself-against-the-heartbleed-bug/.

Arquilla, John. 2002. "Can Information Warfare Ever Be Just?" In J. Rudinow and A. Graybosch, eds. *Ethics and Values in the Information Age*. Belmont CA: Wadsworth, pp. 403–14.

Arrouas, Michelle. 2014. "Change Your Passwords: A Massive Bug Has Put your Details at Risk." *Time*, April 9. Available at: http://time.com/55037/heartbleed-internet-security-encryption-risk/.

Bottis, Maria C. 2007. "Disclosing Software Vulnerabilities." In K. E. Himma, ed. *Internet Security: Hacking, Counterhacking, and Society*. Sudbury MA: Jones and Bartlett, pp. 255–68.

Breitbart, Andrew. 2010. "Google Software Bug Shared Private Online Documents." Available at http://www.breitbart.com/article.php?id=CNG.54c3200980573ae4c.

Cavoukian, Ann. 2008. "Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet." Available at: http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf.

Charette, Robert N. 2012. "Gone Missing: The Public Policy Debate on Unleashing the Dogs of Cyberwar." *IEEE Spectrum*, June 4. Available at http://spectrum.ieee.org/riskfactor/telecom/security/gone-missing-the-public-policy-debate-on-unleashing-the-dogs-of-cyberwar/?utm_source=techalert&utm_medium=email&utm_campaign=060712.

Dale, Nell, and John Lewis. 2016. *Computer Science Illuminated*. 6th ed. Burlington, MA: Jones and Bartlett.

De George, Richard T. 2003. "Post-September 11: Computers, Ethics, and War." *Ethics and Information Technology* 5, no. 4: 183–90.

Denning, Dorothy E. 1999. *Information Warfare and Security*. New York: ACM Press, and Reading MA: Addison Wesley.

Denning, Dorothy E. 2001. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In J. Arquilla and D. Ronfelt, eds. *Networks and Netwars*. Santa Monica CA: Rand Corp., pp. 229–88.

Denning, Dorothy E. 2004. "Cyberterrorism." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 536–41.

Denning, Dorothy E. 2007. "A View of Cyberterrorism Five Years Later." In K. E. Himma, ed. *Internet Security: Hacking, Counter-Hacking, and Society*. Sudbury MA: Jones and Bartlett, pp. 123–29.

Denning, Dorothy E. 2008. "The Ethics of Cyber Conflict." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken NJ: John Wiley & Sons, pp. 407–28.

Epstein, Richard G. 2007. "The Impact of Computer Security Concerns on Software Development." In K. E. Himma, ed. *Internet Security: Hacking, Counter-Hacking, and Society*. Sudbury MA: Jones and Bartlett, pp. 171–202.

Grodzinsky, Francis, S., and Herman T. Tavani. 2011. "Privacy in 'the Cloud': Applying Nissenbaum's Theory of Contextual Integrity." *Computers and Society* 41, no. 1: 38–47.

Himanen, Pekka. 2001. *The Hacker Ethic: A Radical Approach to the Philosophy of Business*. New York: Random House.

Himma, Kenneth Einar. 2007a. "Privacy vs. Security: Why Privacy is Not an Absolute Value or Right," *University of San Diego Law Review* 45: 857–921.

Himma, Kenneth Einar. 2007b. "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?" In K. E. Himma, ed. *Internet Security: Hacking, Counter-Hacking, and Society*. Sudbury MA: Jones and Bartlett, pp. 61–71.

Himma, Kenneth Einar. 2008. "Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken NJ: John Wiley and Sons, pp. 191–217.

Information Warfare Monitor Report. 2009. Available at http://www.nartv.org/mirror/ghostnet.pdf.

Kamlyuk, Vitaly. 2012. "'Flame' Virus Explained: How it Works and Who's Behind it." Interview in *RT*, May 29. Available at http://www.rt.com/news/flame-virus-cyber-war-536/.

Kaufman, Charlie, Radia Perlman, and Mike Speciner. 2002. *Network Security: Private Communication in a Public World*. 2nd ed. Upper Saddle River NJ: Prentice Hall.

Kizza, Joseph M. 2008. *Ethical and Social Issues in the Information Age*. 3rd ed. New York: Springer-Verlag.

Knorr, Eric and Galen Gruman. 2008. "What Cloud Computing Really Means." *InfoWorld*. Available at http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0.

Ladner, Richard. 2012. "Sophisticated Cyber-battles Raise Fears of Cyber-blowback." *MSNBC News*, June 2. Available at http://www.msnbc.msn.com/id/47658329/ns/technology_and_science-security/.

Lawton, George. 2009. "On the Trail of the Conficker Worm." *IEEE Computer* 42, no. 6: 19–22.

Lee, David. 2012. "Flame and Stuxnet Makers 'Co-operated' on Code." *BBC News*, June 11. Available at http://www.bbc.co.uk/news/technology-18393985.

Levy, Steve. 2001. *Hackers: Heroes of the Computer Revolution*. Rev. ed. New York: Penguin.

Lin, Patrick, Fritz Allhoff, and Neill Rowe. 2012. "Is It Possible to Wage a Just Cyberwar?" *The Atlantic*, June 5. Available at http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

Maidment, Paul. 2009. "GhostNet in the Machine." *Forbes.com*. Available at http://www.forbes.com/2009/03/29/ghostnet-computer-security-internet-technology-ghostnet.html.

Manion, Mark and Abby Goodrum. 2004. "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 525–35. Reprinted from *Computers and Society* 30, no. 2 (2000): 14–19.

Mell, Peter and Timothy Grance. 2011. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology. U.S. Department of Commerce. Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Miller, Keith W. 2015. "Malware." In J. Britt Holbrook and C. Mitcham, eds. *Ethics, Science, Technology, and Engineering: A Global Resource*. Vol. 3, 2nd ed. Farmington Hills, MI: Macmillan Reference, pp. 48–52.

Moor, James H. 2001. "Towards a Theory of Privacy for the Information Age." In R. M. Baird, R. Ramsower, and S. E. Rosenbaum, eds. *Cyberethics: Social and Moral Issues in the Computer Age*. Amherst NY: Prometheus Books, pp. 200–12.

Moor, James H. 2004. "Reason, Relativity, and Responsibility in Computer Ethics." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 40–54.

Nakashima, Ellen, and Joby Warrick. 2010. "Stuxnet Was Work of U.S. and Israeli Experts." *The Washington Post*, June 1. Available at http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

National Institute of Standards and Technology. 2011. "The NIST Definition of Cloud Computing." U.S. Department of Commerce. Special Publication 800-145. Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Neumann, Peter G. 2004. "Computer Security and Human Values." In T. W. Bynum and S. Rogerson, eds. *Computer Ethics and Professional Responsibility*. Malden MA: Blackwell, pp. 208–26.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.

O'Harrow, Robert. 2012. "Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks." *The Washington Post*, June 3. Available at http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html.

Pauley, Wayne. 2012. *An Empirical Study of Privacy Risk Methodologies in Cloud Computing Environments*. Dissertation. Nova Southeastern University.

Pieters, Wolter, and Andre van Cleeff. 2009. "The Precautionary Principle in a World of Digital Dependencies." *IEEE Computer Society* 42, no. 8: 50–56.

Privacy Rights Clearing House. 2008. "The Privacy Implications of Cloud Computing." Available at http://www.privacyrights.org/ar/cloud-computing.htm.

Russinovich, Mark. 2005. "Sony, Rootkits, and Digital Rights Management Gone Too Far." Available at http://www.sysinternals.com/blog/2005/10sony-rootkits-and-digital-rights.html.

Sang-Hun, Choe, and John Markoff. 2009. "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *New York Times*, July 9. Available at http://www.nytimes.com/2009/07/09/technology/09cyber.html.

Sanger, David. 2012. "Mutually Assured Cyberdestruction." *New York Times*, June 2. Available at http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html?.

Schneier, Bruce. 2004. *Secrets and Lies: Digital Security in a Networked World*. Rev. ed. New York: John Wiley and Sons.

Simpson, Michael T. 2006. *Hands-On Ethical Hacking and Network Defense*. Boston, MA: Thomson.

Skoudis, Ed. 2004. *Malware: Fighting Malicious Code*. Upper Saddle River, NJ: Prentice Hall.

Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press.

Spafford, Eugene H. 2007. "Are Computer Hacker Break-Ins Ethical?" In K. Himma, ed. *Internet Security: Hacking, Counter-Hacking, and Society*. Sudbury, MA: Jones and Bartlett, pp. 49–59. Reprinted from *Journal of Systems Software*, 17: 41–47.

Spinello, Richard A. 2000. "Information Integrity." In D. Langford, ed. *Internet Ethics*. London, UK: Macmillan Publishers, pp. 158–80.

Spinello, Richard A., and Herman T. Tavani. 2004. "Introduction to Chapter 5: Security and Crime in Cyberspace." In R. A. Spinello and H. T. Tavani, eds. *Readings in Cyberethics*. 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 501–12.

Talbot, David. 2011. "Improving the Security of Cloud Computing," *Technology Review*, June 15. Available at http://www.technologyreview.com/business/37683/.

Tavani, Herman T. 2000. "Privacy and Security." In D. Langford, ed. *Internet Ethics*. London, UK: Macmillan, and New York: St. Martin's Press, pp. 65–95.

Tavani, Herman T. 2007. "The Conceptual and Moral Landscape of Computer Security." In K. E. Himma, ed. *Internet Security: Hacking, Counter-Hacking, and Society*. Sudbury, MA: Jones and Bartlett, pp. 29–45.

Thompson, Paul B. 2001. "Privacy, Secrecy, and Security." *Ethics and Information Technology* 3, no. 1: 13–19.

Viebeck, Elise 2015. "Anarchist Hackers Go to Cyber War with ISIS." *The Hill*, February 12. Available at http://www.msn.com/en-us/news/it-insider/anarchist-hackers-go-to-cyber-war-with-isis/ar-AA9iukK.

Vijayan, Jaikumar. 2012. "Government Role in Stuxnet Could Increase Attacks Against U.S. Firms." *Computer World*, June 2. Available at http://www.computerworld.com/s/article/9227696/Government_role_in_Stuxnet_could_increase_attacks_against_U.S._firms.

Zeng, Ke, and Ann Cavoukian. 2010. *Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach*. Available at: www.privacybydesign.ca.

FURTHER READINGS

Bidgoli, Hossein, ed. 2005. *The Handbook of Information Security*. Hoboken NJ: John Wiley and Sons.

Jordan, Tim. 2008. *Hacking*. Cambridge, UK: Polity Press.

Schneir, Bruce. 2012. *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Hoboken, NJ: John Wiley and Sons.

Tetmeyer, Annette, and Hossein Saiedian. 2010. "Security Threats and Mitigating Risk for USB Devices." *IEEE Technology and Society Magazine* 29, no. 4: 44–49.

Wallace, Kathleen A. 2008. "Online Anonymity." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken NJ: John Wiley and Sons, pp. 165–89.

Wright, Marie, and John Kakalik. 2007. *Information Security: Contemporary Cases*.