Chapter 16

Cybersecurity

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Explain the relationship between cybersecurity and critical infrastructure protections.
- Explain why cyber attack holds so much destructive potential.
- Describe Internet ownership and management relationships.
- Identify key components of the Internet.
- Discuss potential Internet vulnerabilities.
- Evaluate computer crime.
- Describe DHS's cybersecurity roles and responsibilities.

"Because our economy is increasingly reliant upon interdependent cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."

- 1998 Presidential Decision Directive No. 63

Introduction

Cybersecurity goes hand-in-hand with critical infrastructure protection, because 1) cyberspace provides an avenue for attacking critical infrastructure from anywhere around the world; 2) cyber components make critical infrastructure susceptible to subversion, disruption, or destruction; and 3) cyberspace itself is a critical infrastructure on which many other critical infrastructures depend. What keeps the experts awake at night is the knowledge that the potential consequences of a coordinated cyber attack could dwarf any previous disaster in U.S. history, either natural or manmade. This chapter will take a look at some of those nightmare scenarios and examine what the Department of Homeland Security is doing to keep them from becoming reality.

Cybersecurity Concerns: 1) cyberspace provides an avenue for attacking critical infrastructure from anywhere around the world; 2) cyber components make critical infrastructure susceptible to subversion, disruption, or destruction; and 3) cyberspace itself is a critical infrastructure on which many other critical infrastructures depend.

Worst Case Scenarios

The worst disaster in U.S. history was the 1900 hurricane that hit Galveston Texas; as many as 12,000 people are thought to have perished in that disaster. The worst manmade disaster in U.S. history was 9/11 in which 3,000 people lost their lives. [1] Yet the death and damages resulting from these disasters might pale in comparison to the destruction that could conceivably be wrought by a coordinated cyber attack on selected infrastructure. We present just three plausible scenarios that have been considered, at one time or another, at the highest levels of U.S. leadership.

Shutdown the North American Electric Grid.

In August 2003, an electricity blackout affected 50 million people in the northeastern United States and Canada, causing an estimated $4-$10 billion in economic losses. Though it lasted only a week, the outage resulted in a 0.7% drop in Canada's gross domestic product. [2, p. 2] A John Hopkins study determined that New York City experienced a 122% increase in accidental deaths and 25% increase in disease-related deaths, and that ninety people died as a direct result of the power outage. [3] Though the 2003 outage was an accident, it raised concerns whether an even wider outage could be induced deliberately. In 2006, DHS and the Department of Energy conducted a joint experiment named Project Aurora. In this experiment, researchers proved that a generator could be remotely commanded over the Internet to physically self-destruct. [4, p. 21] The implications were shocking because the time necessary to replace a generator can range from months to years. [5, p. 12] Of course the North American electric grid is designed and monitored to sustain service in the event a given component fails. It is not designed, however, to sustain large-scale damages that

might result from a coordinated attack. If such an attack was successful, a significant portion of the United States could lose power for periods lasting months, not weeks. Unlike the aftermath of Hurricane Katrina, there would be no "islands of power" from which to stage recovery or seek refuge. The affected regions would go dark, and their supporting infrastructure would collapse. The cascading effects would be disastrous. No doubt the nation would survive, but it would be deeply wounded as no other experience since the Civil War.

Multiple Simultaneous Meltdowns.

In March 1979, a series of incidents almost resulted in a meltdown of reactor number two at the Three Mile Island nuclear power plant in Dauphin County Pennsylvania. Though a meltdown was averted, and only a slight amount of radiation released, 140,000 people were evacuated from a 20-mile radius before the situation was contained. [6] By comparison, the residents of Pripyat in the Ukraine were not so lucky when in April 1986, reactor number four at the Chernobyl Nuclear Power Plant exploded. Though a different design than the plant at Three Mile Island, the Chernobyl nuclear accident amply demonstrates the dangers of a nuclear meltdown: 350,400 people were permanently evacuated from a radius extending 19-miles in all directions from the plant. Radiation from the fallout is so intense inside the "zone of alienation" that it will remain unsafe for human habitation for another 20,000 years (though a stalwart contingent of 300 residents refuse to leave and remain in the area). [7] Again, these were accidents, but as the Stuxnet attack in 2010 proved, they could conceivably become deliberate. In 2010, the Iranian nuclear program was set back due to production losses at the Natanz uranium enrichment facility. The problem was eventually traced to a piece of malware inserted in Siemens equipment controlling the separation centrifuges. Later called Stuxnet, the malware was extraordinary not only for the damage it caused, but also for how it was implanted. The equipment was not connected to the Internet. The malware had been introduced in the supply chain, somewhere between manufacture and delivery. [8] Stuxnet demonstrates how a similar virus could be concealed inside critical components and timed to initiate a simultaneous meltdown at multiple nuclear power plants. It certainly wouldn't be easy, but it's certainly not improbable.

The death and damages resulting from past national disasters might pale in comparison to the destruction that could conceivably be wrought by a coordinated cyber attack on selected infrastructure.

Shutting Down the Federal Reserve.

The Federal Reserve is the central banking system of the United States. The system is comprised of a Board of Governors, a Federal Open Market Committee, and twelve regional Federal Reserve Banks located in major cities throughout the nation. The Federal Reserve was established in 1913 in response to the financial crisis of 1907 in which payments were disrupted across the country because many banks refused to clear checks drawn on other banks, eventually leading to their failure. To preclude similar panics, the Federal Reserve was formed as a "banker's bank" to facilitate transactions between commercial institutions. Through its actions, the Federal

Reserve influences the availability of money and credit, transacting trillions of dollars underpinning the U.S. economy. [9] The vast majority of these transactions are conducted electronically, between the Reserve Banks and their corporate clients. The system is mostly closed and very well protected, but no defense is invulnerable. Conceivably it could be compromised through a Stuxnet-like attack or by an "insider" attack. An "insider" attack is perpetrated by someone with legitimate access conducting unauthorized actions. Alternatively, a "phishing" attack might trick an authorized user into divulging their access codes to a criminal agent. This last approach is particularly disconcerting because it means system security is only as strong as the weakest person in the chain (of course the computer system has internal as well as external access controls, but accomplished hackers will use their initial access to gain higher authorizations). The potential consequences of a hostile agent shutting down the Federal Reserve are too broad to contemplate. Like electricity, monetary transactions pervade every aspect of society, from ordering a latte to paying the mortgage. What would happen if all forms of electronic payment halted? While you might not be evicted for missing a mortgage payment, you also could not buy that latte, or more importantly, buy gas for your car or groceries for your family. How long would the Federal Reserve have to be down before panic ensued? Not long at all. Again, it's not easy, but it's not impossible.

The Internet is a connected graph of links and routers. What is fundamentally important to the Internet is that each component is independently owned and operated by different public and private agencies: the Internet does not belong to any single entity.

Cyberspace

As explained in the introduction, cyberspace serves as both an avenue of attack and a means of support for other critical infrastructure. Understanding what it is, therefore, is an important precondition to protecting it. According to the DHS Glossary of Common Cybersecurity Terminology, cyberspace is "the interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers." [10] Essentially "cyberspace" is a broad term encompassing the Internet and everything connected to it. So what is the Internet? By definition the Internet is a "network of networks". The key enabling technologies are links, standards, protocols, and routers. A link is a physical communications path between two points. A link may be wired (copper or fiber) or wireless (light or radio), depending on required cost, distance, and bandwidth. A link serves to transmit electronic data packets conforming to the Open System Interconnection (OSI) standard. The source and destination of each data packet are internally encoded in a globally unique Internet Protocol (IP) address. A link may terminate at a router, which, in turn, may be connected to two or more links. A router examines the destination address of each arriving packet and forwards it on to another link to convey it closer or quicker to its final destination. It may require many packets to transmit a single text, graphic, sound, or video object. The Transmission Control Protocol (TCP) ensures that all packets are properly re-assembled into the

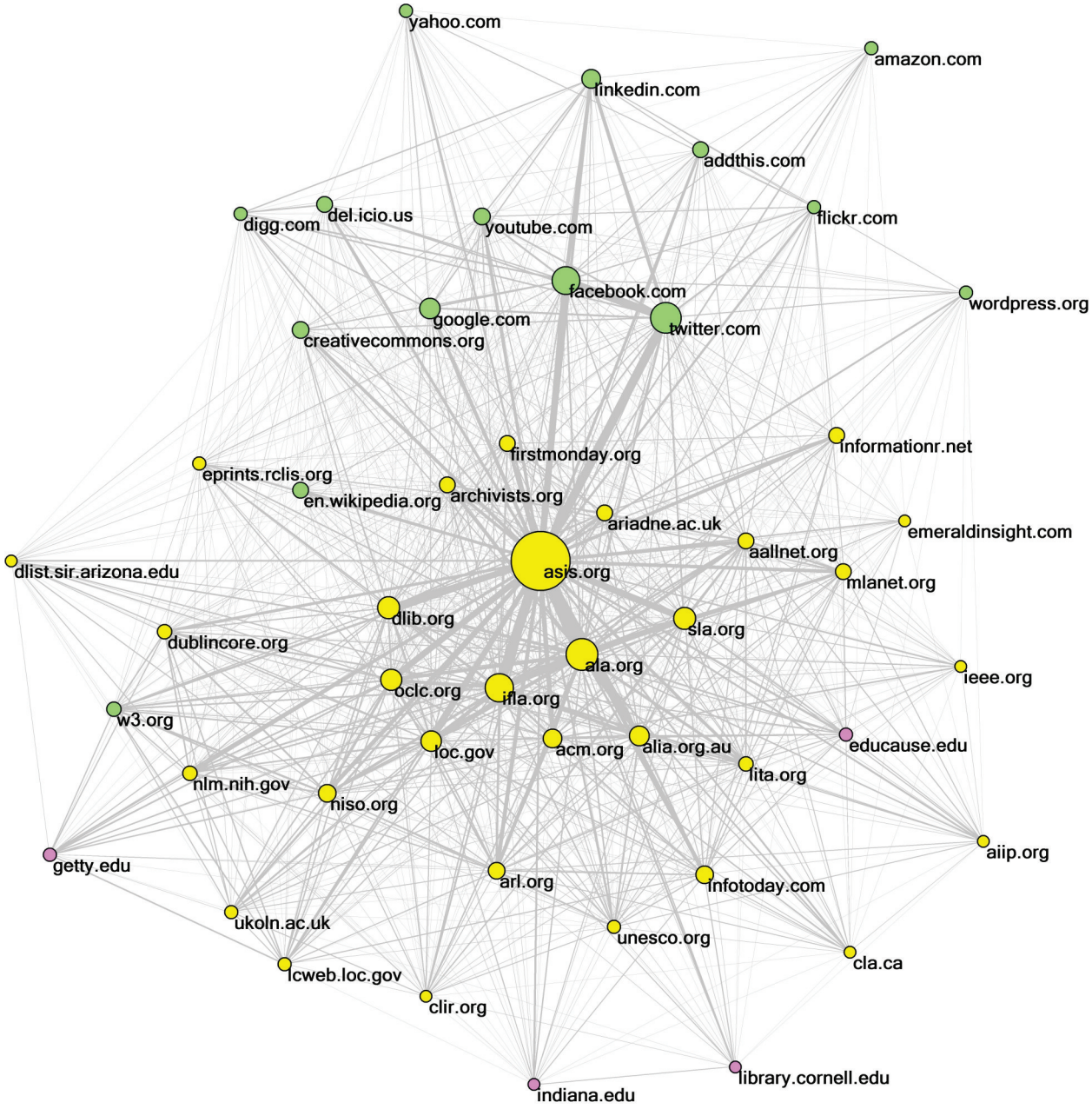

Figure 16-1: Schematic Representation of a Portion of the Internet

original object at their intended destination[1]. While greatly simplified and highly abstract, the preceding description provides a physical conception of the Internet, which may be schematically represented as shown in Figure 1.

As shown in Figure 1, the Internet is a connected graph of links and routers. What is not shown, and what is fundamentally important to the Internet, is that each component is independently owned and operated by different public and private agencies: the Internet does not belong to any single entity. It is a collection of diverse

[1]A "message" may be digitized text, graphics, sound, or video. Sound and video packets may be transmitted using the User Datagram Protocol (UDP) which trades speed for reliability compared to TCP. A few lost sound or video packets will not be discernable to the human ear or eye.

components conforming to an agreed set of engineering standards. The individual owners are collectively called Internet Service Providers (ISPs). The Internet is built and grows as ISPs join their networks with those of other ISPs.

ISPs are unofficially classified into "Tiers" based on the size of their networks and how they connect with other ISPs. ISPs connect to each other through either a "peering" or "transit" agreement. Peering is when a pair of ISPs establish a reciprocal agreement to connect with each other and exchange traffic without charge. On the other hand, a transit relationship requires some form of fee based on the amount of traffic shared between the ISPs. [11] Accordingly, ISPs are classified as Tier 1, Tier 2, or Tier 3. Tier 1 ISPs are the largest, and peer with other Tier 1 ISPs to reach every other ISP on the Internet without purchasing transit. Table 1 lists the seven U.S. Tier 1 ISPs. Tier 2 ISPs peer with some ISPs, but purchase transit to reach at least some portion of the Internet. Examples of Tier 2 ISPs are major cable, Digital Service Link (DSL), and mobile providers. Tier 3 ISPs must purchase transit from other ISPs to access the Internet. Examples of Tier 3 ISPs are small regional providers, small mobile providers, and university networks. [12]

The individual owners are collectively called Internet Service Providers (ISPs). The Internet is built and grows as ISPs join their networks with those of other ISPs.

Table 16-1: U.S. Tier 1 ISPs [13]

1.	AT&T	5.	Level 3
2.	Verizon	6.	NTT/Verio
3.	Spring	7.	Cogent
4.	Century Link		

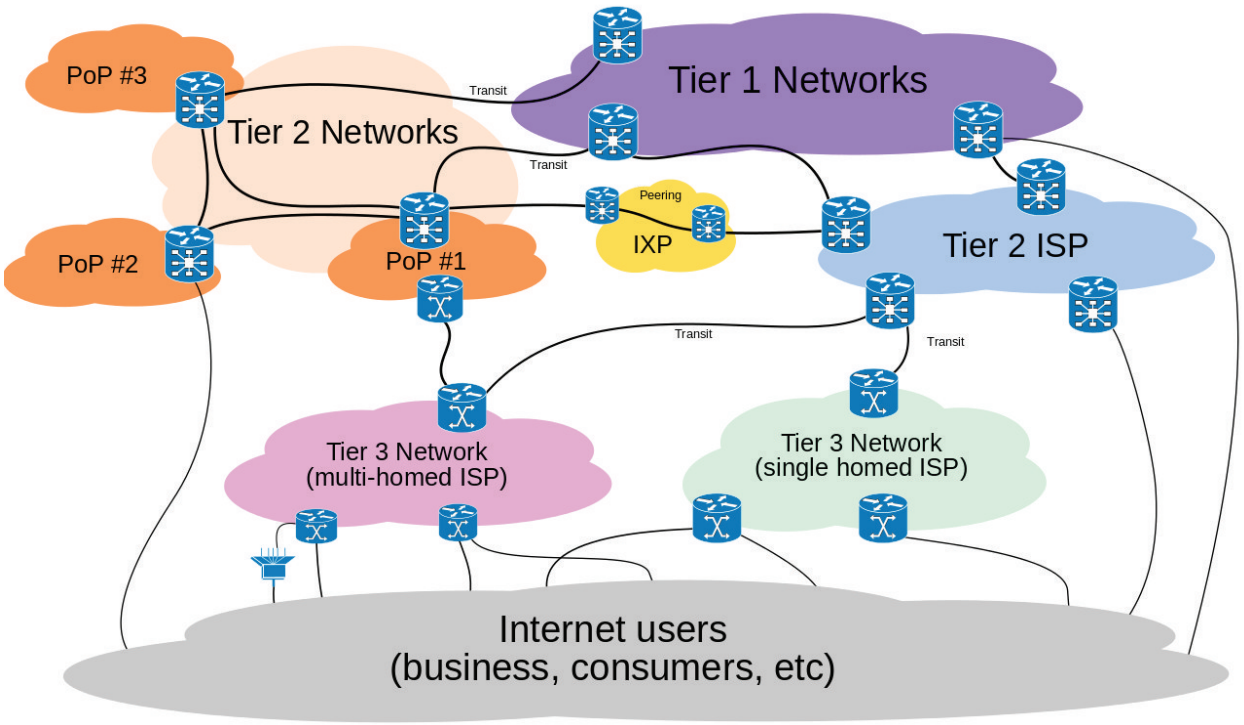

Figure 16-2: Internet ISP Tiers

Transiting and peering between ISPs is facilitated by Internet Exchange Points (IXPs). The primary role of an IXP is to keep local traffic local and reduce the costs associated with traffic exchange between Internet providers. IXPs are a vital part of the Internet. Without them, the Internet would not function efficiently because the different networks that make up the Internet would need to directly interconnect with every other network in order to be able to exchange traffic with each other. [15]

The compelling benefits of IXPs spurred their rapid global growth. As of 2012, there were 350 IXPs operational worldwide. The US has about 86 IXPs strategically located across the country. Other countries with more than 10 IXPs are: Australia (11), Brazil (19), France (15), Germany (14), Japan (16), Russia (14), Sweden (12), and United Kingdom (12). [15]

Internet Exchange Points (IXPs) are a vital part of the Internet. Without them, the Internet would not function efficiently because the different networks that make up the Internet would need to directly interconnect with every other network in order to be able to exchange traffic with each other.

As mentioned previously, the Internet is not owned by any single entity, however, it does rely on central services to ensure unique Internet Protocol addresses for each component connected to it. IP addresses are controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a global non-profit agency operating out of Los Angeles California. IP addresses come in two forms: 1) human-readable, i.e., "alias", and 2) machine-readable, i.e., "numeric". While the human-readable address is easier for people to remember (e.g., facebook.com, Google.com, Amazon.com), the machine-readable address is the form required by routers (e.g., 173.252.120.6, 74.125.70.102, 72.21.215.232). Accordingly, the Internet relies on

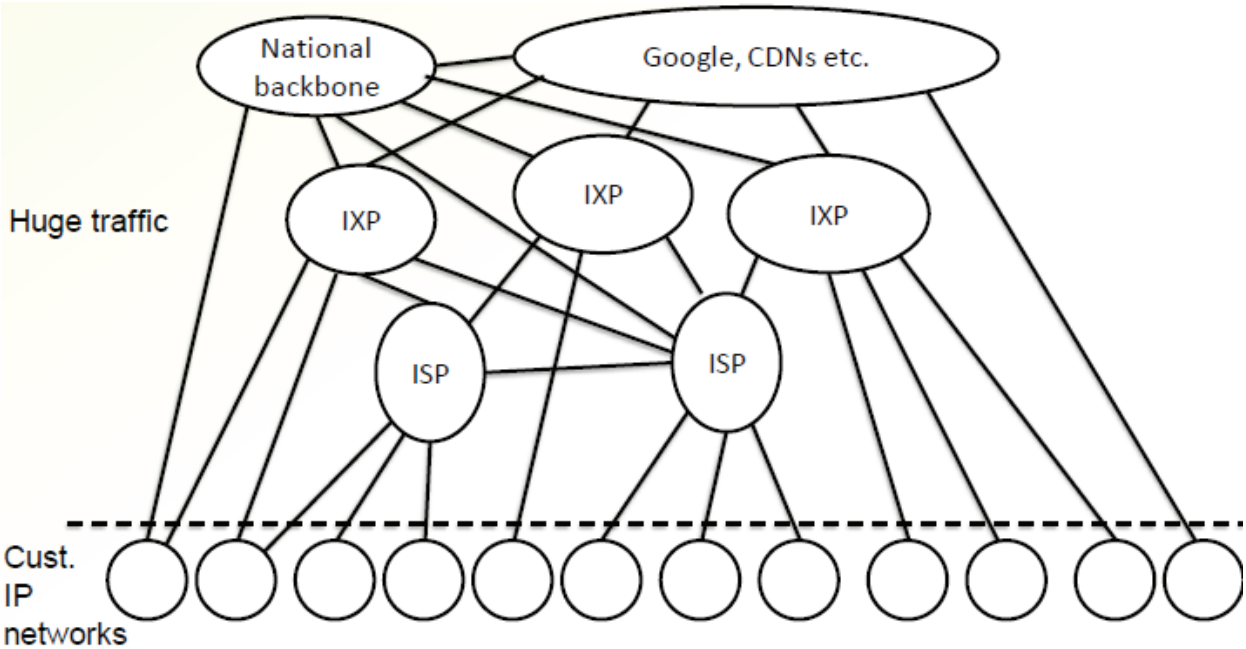

Figure 16-3: IXP Role in Today's Internet [16]

Domain Name Services (DNS) to translate one form of IP address into another and help route traffic along the Internet. DNS is maintained by a department of ICANN called the Internet Assigned Numbers Authority (IANA). IANA operates and maintains DNS services provided by hundreds of computers known as root servers located in many countries in every region of the world. Root servers contain the IP addresses of all the Top-Level Domain (TLD) registry name servers; e.g., ".com" and ".de". Root servers "translate" aliases into numbers. They perform a critical if somewhat "back-office" role in ensuring the continuity and therefore reliability of the Internet. [17]

Cyber Attack

The 1984 Counterfeit Access Device and Computer Fraud & Abuse Act (18 USC S1030) prohibits unauthorized access to computers used by the Federal government, banks, and otherwise used for interstate or international commerce. Due to the inter-state nature of the Internet, the law is interpreted to mean most all computers including cell phones.

The 1984 Counterfeit Access Device and Computer Fraud & Abuse Act (18 USC S1030) prohibits unauthorized access to computers used by the Federal government, banks, and otherwise used for interstate or international commerce. Due to the inter-state nature of the Internet, the law is interpreted to mean most all computers including cell phones. A 1986 amendment further criminalized the distribution of malicious code, trafficking in passwords, and denial of service attacks. [18] According to the U.S. National Research Council, a cyber attack is any "deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and /or programs resident in or transiting these systems or networks." [19, p. 9] There are many different ways to mount a cyber attack as illustrated in Figure 4. According to a 2014 report by the Center for Strategic and International Studies, the two most common attack methods are social engineering and vulnerability exploitation. According to the Center, social engineering is where an attacker tricks a user into granting access, and vulnerability exploitation is where an attacker takes advantage of a programming or implementation failure to gain access. [20, p. 10] According to the report, cybercrime is a growth industry because the returns are great and the risks are low. The Center estimates that the annual cost to the global economy is more than $400 billion, yet most cybercrime goes unreported, and few cybercriminals are caught or even identified. [20, p. 2&4]

Cyber Security

The DHS Glossary of Common Cybersecurity Terminology defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. [10] Cybersecurity is also a growth industry. According to the Center for Strategic and International Studies, the global market for cybersecurity products and services is $58 billion and growing annually. [20, p. 17] In concept, cybersecurity is very simple. All you have to do is ensure the confidentiality, integrity, and availability of the computer system and its data. Confidentiality ensures the system and data are not accessed by an unauthorized agent. Integrity ensures that the system and data are not corrupted by an unauthorized agent. Availability ensures that the system and data are always

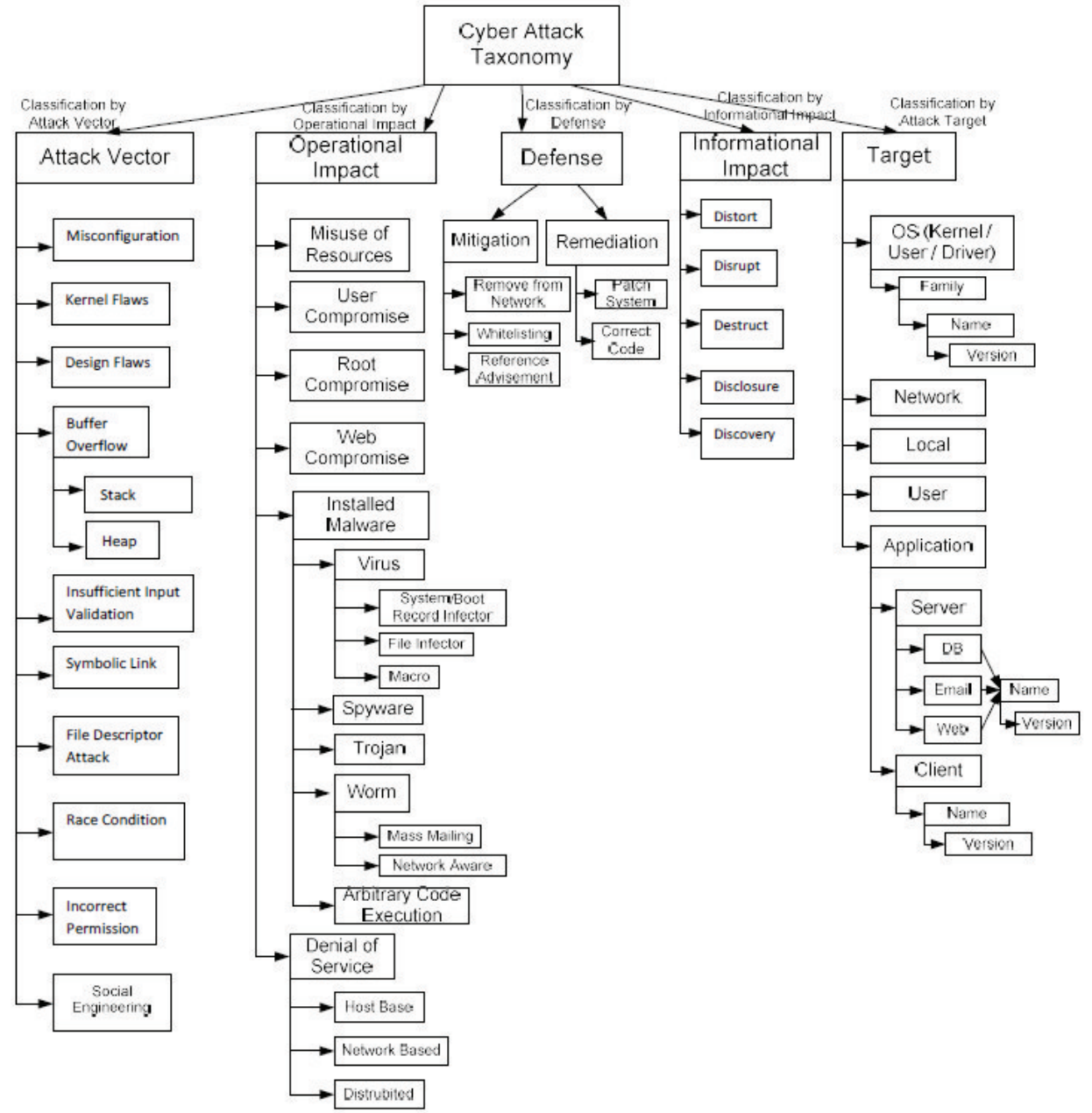

Figure 16-4: AVOIDIT Cyber Attack Taxonomy [23]

accessible when needed. [21, pp. 1-2] These seemingly simple goals, however, are very difficult to attain because computers are inherently stupid and fragile. Computers are stupid, because unlike humans, computers are incapable of making value judgments regarding their actions and will perform as directed regardless of outcome, even if the consequences are catastrophic. Computers are also fragile; a single wrong character can disrupt millions of lines of code, compared to buildings which do not collapse because one brick fails. Finding such flaws is impossible. Even a small 100-line program with some nested paths and a single loop executing less than twenty times may contain 100 trillion paths. Assuming each path could be evaluated in a millisecond (one-thousandth of a second), testing would take 3170 years. [22] The cumulative effect makes computers inherently vulnerable to diversion from their intended purpose, either through oversight or tampering.

Protecting Cyberspace

Section 103 of the Homeland Security Act made the Department of Homeland Security responsible for cybersecurity at the same time it made it responsible for critical infrastructure protection. [24] As an infrastructure, the Internet underpins the functioning of most other infrastructures, making it essential to the economy and security of the United States. [25, p. 1] Although the Internet is comprised of billions of components globally, it depends on only a thousand to maintain proper functioning, offering a relatively small set of lucrative targets capable of incapacitating the Internet. These include the Internet Exchange Points and DNS Root Servers. Any number of attacks could possibly be launched and some have already been attempted against these high-value assets. In October 2002, a Distributed Denial of Service (DDoS) attack succeeded in affecting 9 of 13 root servers, and at least two root servers "suffered badly" from another attack in February 2007. [26] Because IXPs are designed to manage large traffic loads, a specific type of DDoS attack called a Cross-Plane Session Termination (CXPST) attack employing about 250,000 "bots" would be needed. It is surmised that a well targeted and well timed attack could take down significant parts of the Internet. [16, p. 48]

Although the Internet is comprised of billions of components globally, it depends on only a thousand to maintain proper functioning, offering a relatively small set of lucrative targets capable of incapacitating the Internet. These include the Internet Exchange Points and DNS Root Servers.

As an infrastructure, the Internet is included in the DHS National Infrastructure Protection Plan (NIPP). The DHS National Cyber Security Division (NCSD) under the Office of Cybersecurity and Communications (CS&C) is the Sector Specific Agency (SSA) for the Information Technology (IT) Sector. DHS has no regulatory authority over the IT sector. NCSD, therefore, works in voluntary cooperation with private partners in the Sector Coordinating Council (SCC), including some Tier 1 Internet Service Providers listed in Table 1. As part of the NIPP, DHS supports an IT Information Sharing and Analysis Center (IT-ISAC) to promote the exchange of threat and security information among SCC partners. Private organizations may also report cyber incidents to the DHS National Incident Coordinating Center (NICC). In 2010, NCSD worked with sector partners to produce the IT Sector Specific Plan (IT-SSP). The 2010 IT-SSP reported the results of a 2008-2009 IT Sector Baseline Risk Assessment (ITSRA), noting concerns about DNS root services. [27] ITSRA appears to be a one-off study, conducted as the NIPP Risk Management Framework (RMF) was still gaining traction. In May 2013, DHS noted the use of an NCSD-developed Cyber Assessment Risk Management Approach (CARMA) for conducting risk assessment of cyber assets in conjunction with the NIPP Risk Management Framework. [28]

The basic problem of the Internet is that it is a victim of its own success. Originally designed as a research tool for a trusted community of researchers, the Internet has expanded well beyond its original design specifications and must today operate in an environment that cannot be trusted.

Protecting Infrastructure from Cyberspace

Many critical infrastructures including electricity transmission systems, gas pipelines, and water distribution systems rely on Industrial Control Systems (ICSs) to monitor and control physical objects and devices, such as switches and valves that are often located in remote locations. Industrial Control Systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), and General-Purpose Controllers (GPCs). Most ICSs began as proprietary, stand-alone systems that were separated from the rest of the world and isolated from most external sources. Today, widely available software applications, Internet-enabled devices and other nonproprietary information technology offerings have been integrated into most ICSs. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems to malicious attacks, equipment failures, and other threats. ICS disruptions or failure can result in death or injury, property damage, and loss of critical services. [29]

Industrial Control Systems present a particularly worrisome problem as a coordinated attack might result in some form of worst case scenario. Accordingly, in 2010 DHS released a National Cyber Incident Response Plan (NCIRP) describing how it would prepare for, respond to, and begin to coordinate recovery from a significant cyber incident.

In 2004, the Department of Homeland Security's National Cybersecurity Division established the Control Systems Security Program (CSSP), which was chartered to work with control systems security stakeholders through awareness and outreach programs that encourage and support coordinated control systems security enhancement efforts. In 2009, the CSSP established the Industrial Control System Joint Working Group (ICSJWG) as a coordination body to facilitate the collaboration of control system stakeholders and to encourage the design, development and deployment of enhanced security for control systems. In 2011, the ICSJWG released a Cross-Sector Roadmap for Cybersecurity. [29]

Industrial Control Systems present a particularly worrisome problem as a coordinated attack might result in some form of worst case scenario examined at the beginning of this chapter. Accordingly, in 2010 DHS released a National Cyber Incident Response Plan (NCIRP) describing how it would prepare for, respond to, and begin to coordinate recovery from a significant cyber incident. A significant cyber incident is classified as a Level 2, "substantial" incident on the National Cyber Risk Alert Level (NCRAL) shown in Table 2. Threat levels are monitored at the DHS National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour operations center ready to coordinate a national cyber incident response. Among its assets, the NCCIC has access to both the US-CERT and ICS-CERT. [30]

Table 16-2: DHS National Cyber Risk Alert Levels

Level	Label	Risk	Response
1	Severe	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential
2	Substantial	Observed or imminent degradation of critical functions with moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The DHS Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber Unified Command Group take place. Other similar non-Federal incident response mechanisms are engaged
3	Elevated	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slight enhanced, operational posture
4	Guarded	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation

U.S. Computer Emergency Readiness Team (US-CERT). US-CERT is a partnership between DHS and the public and private sectors. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration among State, Local, Tribal and Territorial governments, industry, and international partners. US-CERT interacts with Federal agencies, industry, the research community, State, Local, Tribal and Territorial governments, and other entities to disseminate reasoned and actionable cybersecurity information to the public. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. Government about cybersecurity. [30, pp. N-2]

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT provides focused operational capabilities for defending control system environments against emerging cyber threats. ICS-CERT provides efficient coordination of control systems-related security incidents and information sharing with Federal, State, Local, Tribal and Territorial agencies and organizations; the Intelligence Community (IC); private sector constituents, including vendors, owners, and operators; and international and private sector CERTs. ICS-CERT leads this effort by responding to and analyzing control systems-related incidents, conducting vulnerability and malware analysis, providing onsite support for forensic investigations, and providing situational awareness in the form of actionable intelligence and reports. [30, pp. N-2]

The DHS NCCIC primarily serves as a warning and alerting system. While the US-CERT and ICS-CERT may provide analysis and recommendations, DHS does not have deployable cyber units that will show up onsite and fix your cyber problems. The closest such capability is being built by the Department of Defense (DoD) as part of their National Cyber Mission Force (CMF) promulgated under the DoD's Cyber Strategy. The DoD Cyber Strategy has three missions: 1) defend DoD networks, systems, and information; 2) defend the U.S. homeland and U.S. national interests against cyber attacks of significant consequence; and 3) provide cyber support to military operational and contingency plans. Towards this end, DoD will develop 68 Cyber Protection Teams (CPTs) to perform the first mission; 13 National Mission Teams (NMTs) for the second mission; 27 Combat Mission Teams (CMTs) for the third mission; and 25 National Support Teams (NSTs) to assist them all. [31]

The DHS National Cybersecurity and Communications Integration Center (NCCIC) primarily serves as a warning and alerting system. While the US-CERT and ICS-CERT may provide analysis and recommendations, DHS does not have deployable cyber units that will show up onsite and fix your cyber problems.

The 13 National Mission Teams comprising the National Mission Force (NMF) will be supported by 8 NSTs (also called Direct Support Teams), and will be designed to defend the nation against strategic cyber attacks on U.S. interests. Reportedly, the NMTs will employ counter-cyber force to stop cyber attacks and malicious cyber activity of significant consequences against the nation. [32, p. 9]

While details remain sketchy, it appears the NMTs will only be employed in the case of foreign cyber attack. Attribution is a thorny problem when it comes to cyber attack. As was already mentioned, few cyber criminals are identified let alone caught. The implication is that NMTs will have very limited domestic utility, and there will be no cyber cavalry coming to the rescue in the event of a significant domestic cyber attack. Ultimately, infrastructure owners/operators must rely on their own devices to protect their assets.

Protecting Cyber Assets

In February 2013, President Obama signed EO 13636, Improving Critical Infrastructure Cybersecurity, assigning the National Institute of Standards and Technology (NIST) responsibility for developing a Cybersecurity Framework. The framework was to form the basis for a Voluntary Critical Infrastructure Cybersecurity Program that would encourage critical infrastructure owners and operators to improve the security of their information networks. NIST released Version 1.0 of the Framework February 12, 2014. [33, p. 13]

EO 13636 also required those agencies with regulatory authority over certain critical infrastructure owner and operators to evaluate whether "the agency has clear authority to establish requirements… to sufficiently address current and project cyber risks to critical infrastructure." Although DHS has no regulatory authority over Internet Service Providers, as the Sector Specific Agency DHS recommended voluntary application of cybersecurity measures for the Information Technology sector. [34]

The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. [35]

In February 2013, President Obama signed EO 13636 directing the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework. A year later, NIST released v1.0 of a framework that was to form the basis of a Voluntary Cybersecurity Program encouraging critical infrastructure owners and operators to improve the

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory. [35]

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. [35]

A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations. [35]

While the NIST Cybersecurity Framework doesn't explain how, it is assumed that an asset's profile can be mapped to a tier level. Presumably the higher the tier level, the more secure the asset. But this is all about risk management, so there are no guarantees.

Conclusion

Cybersecurity as a mission of homeland security has come full circle. Recognizing that the growing use of the Internet portended a potential avenue of attack, the 1997 Report of the President's Commission on Critical Infrastructure can be considered the beginning of homeland security. PDD-63 laid the foundation for the critical infrastructure protection mission. Whereas PDD-63 was focused on cyber threats to infrastructure, HSPD-7 understandably gave priority to physical threats after the example of 9/11. In response to the growing frequency and ferocity of cyber attacks on the nation, PPD-21 restored the primacy of cybersecurity to homeland security. Cybersecurity and critical infrastructure protection are inseparable. Aware of the potential worst case scenarios, today we remain an ever vigilant nation against cyber attack.

Challenge Your Understanding

The following questions are designed to challenge your understanding of the material presented in this chapter. Some questions may require additional research outside this book in order to provide a complete answer.

1. How is cybersecurity related to critical infrastructure protection?
2. Why does cyber attack hold so much destructive potential?
3. Of the possible worst case scenarios, which do you think would be most devastating? Explain.
4. Of the possible worst case scenarios, which do you think would be most long lasting? Explain.
5. Who owns the Internet?
6. Who manages the Internet?
7. According to the 1984 Counterfeit Access Device and Computer Fraud & Abuse Act, which of the following actions constitute a crime?
    a. Accessing a computer without the owner's consent.
    b. Probing a network to assess its security measures.
    c. Disconnecting the Internet to contain a virus.
8. List and describe two potential targets that could shutdown the Internet.
9. What is DHS's role in cybersecurity?
10. How many cyber teams does DHS have ready to deploy in the event of a national emergency?

Chapter 17

Counterterrorism

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Explain how terrorism uniquely distinguishes the crime of assault.
- Explain why Islamic extremism is considered a terrorist threat.
- Evaluate the 2011 National Strategy for Counterterrorism.
- Assess the different roles of the FBI and DHS under PDD-39/HSPD-5.
- Discuss the primary means for dealing with known terrorists, foreign or domestic.
- Compare different options for dealing with foreign terrorists.