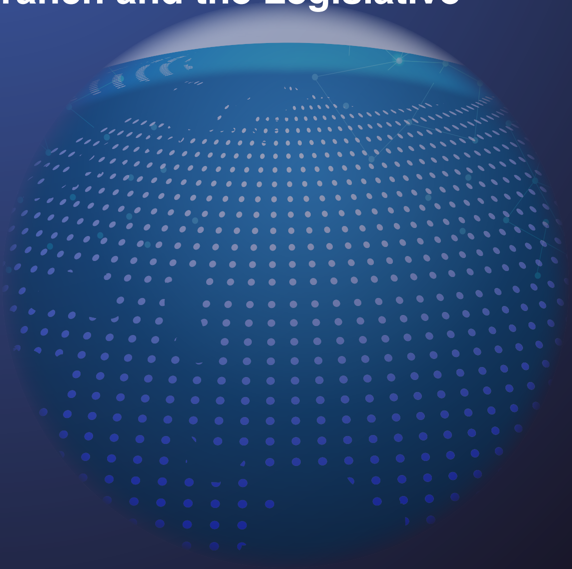
CYBERSECURITY
FOUNDATIONS
AN INTERDISCIPLINARY INTRODUCTION

CHAPTER 6: Advanced Cybersecurity Studies: Research Methods and Sources

CHAPTER OUTLINE

- Overview of Advanced Cybersecurity Studies: Research Methods and Sources
- Introduction to Research Methods
- The U.S. Constitution and the Three Branches of Government
- The Role of the Executive Branch
- The Role of the Legislature
- Federal Regulations: The Executive Branch and the Legislative Branch Combined
- The Role of the Judiciary
- Cybersecurity: A Global Perspective
- Conclusion
- Key Questions



6 Advanced Cybersecurity Studies: Research Methods and Sources

Chapter In Focus

- Research methods and how to apply them.
- Researching executive, legislative and judicial sources.
- Federal regulations as sources.
- Research methods and sources on the global scale.
- Cybersecurity in the international community.

Overview of Advanced Cybersecurity Studies: Research Methods and Sources

As this book has demonstrated, cybersecurity is truly an interdisciplinary field. Therefore, delving deeper into cybersecurity problems and proposing new policies and solutions requires a flexible and interdisciplinary approach to academic research. Potential research topics in the field may come from subfields as varied as cyber risk management, cyber law and policy, cybersecurity program management, cybersecurity technology, and cybersecurity for the private sector. Researchers in cybersecurity may pursue new breakthroughs in any of these topics, or create new frameworks, theories, policies, and plans that combine knowledge generated from two or more fields.

Domestic and international events, institutions, and technological developments drive new developments in cybersecurity research. For example, the crippling 2007 cyber attacks against Estonia's banks, media, and government, the United States' deployment of the Stuxnet worm against Iran's nuclear facilities, and the appearance of the highly complex Flame worm in Middle Eastern critical infrastructure computer systems, are all events that have shaped new cybersecurity methods, policies, and technologies. Thus, the discussions, debates, official policies, new government programs, and technological projects that follow any cybersecurity incident, particularly those that occur on a massive scale, have become rich areas for researchers to investigate and analyze.

National governments and international institutions produce documents of great interest to cybersecurity researchers. In part because the Internet began as a project of the DOD, the U.S. government remains the world's leading institution in the development of cybersecurity law, policy, technology, and research. Moreover, U.S. government documentation of cybersecurity policies, proposals, strategies, debates, legislation, and regulation has served as an invaluable model for other national governments and for the private sector.

A researcher's access to databases and documents is not enough to generate original contributions to the field, however; researchers must begin their investigations by understanding the authorities, processes, histories, and problems that inform these research sources. This chapter will ground you in the practice of researching cybersecurity problems by introducing you to some of the organizations and institutions where these problems are most often discussed, analyzed, and tackled. This chapter will guide you through the structure and policymaking process of the U.S. government as it relates to cybersecurity, and then examine the role of international institutions.

Finally, it is important to note that academics, intellectuals, and students are not the only people who pose research questions and conduct research. The information in this chapter will benefit both public and private-sector professionals who work on cybersecurity problems in any capacity.

Introduction to Research Methods

As an academic discipline, cybersecurity is a unique fusion of computer science, law and policy, risk management, business, and program management. However a researcher approaches a cybersecurity problem, he will inevitably encounter more than one of these areas of study (in this section, we will assume that our hypothetical researcher is male). But even though cybersecurity is an interdisciplinary field, the researcher's focus must be narrow enough to study, test, and analyze a specific subject.

Besides these potential areas of research, the academic field of cybersecurity has also given rise to a growing collection of theories. **Theories** in this context are statements that have been tested repeatedly and accepted by experts. Rigorous hypothesis testing and research can challenge established theories, propose new theories, and add to the complexity and scope of cybersecurity as an academic discipline.

Therefore, for students contemplating careers in cybersecurity, the challenge is both what to study and how to study it. **Ontology** is the theory of being, or what is being studied or researched. **Epistemology** is the theory of knowledge, or how an event, phenomenon or object is studied, researched, analyzed, and understood. The epistemology of a research project is the project's guiding philosophy about the best way to produce new knowledge.

Once the researcher has determined the epistemological and ontological reference for his work, he can determine the research design that his project will follow. A **research design** is the outline of the research—a complete blueprint for how the researcher will attempt to answer the question posed by his project. There are two kinds of research design: *experimental* (in which the researcher runs an experiment) and *nonexperimental* (in which there is no experiment). Both types of research design may involve a mixture of quantitative and qualitative methods. The type of research design is contingent on the question the researcher posed at the beginning of the project.

Research questions often focus on the main theoretical debates or unanswered questions in a field. Therefore, in cybersecurity, a researcher may examine the debates raised by historical events, judicial precedents, relevant legislation, new policies, and technological advancements. For example, a researcher might ask: "Which U.S. cybersecurity laws and regulations have had the greatest influence on international cybersecurity standards?" Or: "What privacy concerns have been raised by the ability of telecommunications companies to monitor Internet traffic?"

Neither of these cybersecurity research questions would necessarily require the researcher to run an experiment. Experimental research is relatively rare in cybersecurity because it requires the researcher to have total control of the experiment's independent variables. **Independent variables** are the factors that influence outcomes, the **dependent variables**. For example, the growth of a plant is dependent on the plant's exposure to sunlight; thus, growth of the plant is the dependent variable (y), and exposure to the sun is an independent variable (x).

Cybersecurity experiments follow a similar design. For example, researchers may run experiments to test the effectiveness of a new antivirus software or IDS. The researcher's choice to include or omit relevant factors that can influence the outcome will determine whether or not the results are relevant and whether or not the experiment is successful. A successful experiment will be able to show that a meaningful relationship between one or more variables either does or does not exist.

Nonexperimental research is more common in the social sciences. In this type of design, the researcher does not have control over all of the independent variables, and there is only one test group. In most cases, nonexperimental research involves studying a subject "as is," rather than running an experiment upon it. Examples of common nonexperimental research subjects include human behavior, literature, and history.

There are three types of nonexperimental research: exploratory, explanatory, and descriptive. *Exploratory research* provides preliminary concepts and findings about an underdeveloped topic and establishes a baseline for future study. Small focus groups or open-ended interviews with limited participants are examples of exploratory research.

Explanatory research attempts to answer a "why" question. Explanatory researchers may engage in rigorous hypothesis-testing in order to determine a relationship between two or more variables. The case study in Chapter 1 involving an online retailer trying to protect its network from a cyber attack is an example of explanatory research, in which the researcher examined which combination of security controls yielded the most secure website. In this type of research, researchers may manipulate a dataset to test the effect of various independent variables on the dependent variable. Explanatory research cannot prove a causal relationship, but it can prove or disprove a significant relationship between multiple variables.

Descriptive research provides more details than exploratory research, and its results may be more generalizable. Large-sample surveys are examples of descriptive research. Descriptive research does not typically employ hypothesis testing.

Applying Research Methods

This chapter will examine the events, official statements, legislation, publications, international organizations, and other sources that have shaped cybersecurity policy and thought. These sources are all potential **units of analysis**, or research subjects. For new researchers, deciding exactly what question or problem to research, then further refining the research focus, can be a difficult and time-consuming process. Still, the more specific the question a researcher poses at the beginning of an investigation, the easier it will be to choose the most relevant variables, create hypotheses, perform research, analyze the results, and draw conclusions that contribute new knowledge to the field.

As these five steps suggest, even in a nonexperimental research project, the researcher must strive to conduct research with the strict objectivity and step-by-step approach of a scientist. In other words, the basic principles of the **scientific method**—systematic and objective examination of a phenomenon—apply to the work of cybersecurity researchers.

After the researcher selects his unit of analysis, he must decide on the **time dimension** for the research—the precise time period the researcher will investigate. Determining the time dimension establishes a boundary for the scope of the unit of analysis. Once the researcher has narrowed the research question and established the units of analysis and time dimension, he can begin to develop hypotheses, if the project calls for hypothesis testing.

Throughout the research design phase, the researcher should conduct validity and reliability tests. **Validity** means that the researcher is testing precisely the variables and subjects he set out to study; **reliability** means that another researcher could replicate the design and reach the same results. Testing for validity can be difficult in an interdisciplinary field like cybersecurity, as it can sometimes be hard to determine which sources pertain directly to the research question and which do not. In terms of reliability, the success of the researcher's project will depend on how strictly he has adhered to the scientific method throughout the project.

The researcher must be careful to avoid common mistakes of logic and reasoning when examining, analyzing, and drawing conclusions about his subject. Mistakes of logic and reasoning can undermine a good research question and render an entire research design useless. Common logical mistakes involve logical fallacies. **Logical fallacies** are statements that are based on some kind of misconception. Researchers may unwittingly commit logical fallacies when they make statements that fail to adhere to the rules of logic.

For example, the *ecological fallacy* occurs when the researcher assumes that a fact or relationship that is true for one sample is true for another, typically larger, sample or unit of analysis. The *genetic fallacy* occurs when a researcher rejects an idea based on its origin rather than its merit. The *bandwagon fallacy* occurs when a researcher accepts an idea as true because it is increasing in popularity, and the complex question fallacy occurs at the very beginning of a research project, when a researcher poses a question that depends on a questionable assumption.

Researching Cybersecurity through U.S. Government Documents

The U.S. government is a massive organization that has committed billions of dollars to a long-term cybersecurity effort. The U.S. government's investment in the development of cybersecurity thought, technology, law, and policy is considered a benchmark for the rest of the world. For this reason, this chapter will focus on U.S. government cybersecurity sources, which can inform and strengthen cybersecurity research on any topic.

In any research project, the researcher may need to consult an enormous number of sources related to the U.S. federal government: White House directives and memoranda, federal agency regulations and guidance, legislation and its history, case studies of federally prosecuted cyber crimes, and guidelines for judges to sentence cyber criminals. These sources are only the beginning of a growing list.

Cyber Fact

In Chapter 2 (Cybersecurity Law and Policy), we discussed in detail how catastrophic events can trigger significant policy changes within the highest levels of the U.S. federal government. After the Oklahoma City bombing in 1995 and terrorist attacks of September 11, 2001, national security experts predicted that a massive cyber attack could cripple the domestic economy if the federal government failed to secure its digital infrastructure. As a result, cybersecurity became one of the leading issues in discussions of U.S. national security.

The U.S. Constitution and the Three Branches of Government: Establishing Power to Produce and Enforce Federal Laws

The Constitution of the United States guides the actions of the federal government. In its first three articles, the Constitution created the legislative (U.S. Congress), executive (U.S. president), and judicial (U.S. federal courts) branches of the federal government. The different roles played by the three branches of government in the formation of national cybersecurity policy have produced contrasting types of cybersecurity documents and cybersecurity ideas.

For example, in both appearance and power, a presidential directive is significantly different from a piece of congressional legislation or a Supreme Court decision. In your research on existing and developing cybersecurity issues, you will need to know the difference between the types of documents that each branch of government produces, as well as the different kinds of power that each branch has to create and enforce laws and policies. As you move beyond the U.S. in your cybersecurity research, you will also need to know about the types of cybersecurity work performed by internationally oriented research bodies, such as the IETF, and by global security organizations, such as the United Nations (U.N.) and NATO.

One consistent theme you will encounter in this chapter is that new cyber laws and policies tend to originate in the executive branch of the U.S. federal government. Because the executive branch has the role of "first responder" during national security emergencies, and because national security emergencies often precede new national security policies, new cybersecurity policies naturally flow from the executive branch. These executive policies, issued in executive orders and national security instruments (such as NSDDs, PDDs, NSPDs, etc.), apply to the U.S. government's federal departments and agencies and in this way influence the day-to-day operations of the federal government. In order for presidential policies to take on a broader application, they must be passed into law and funded by the U.S. Congress.

The Role of Congress in Executive Policies

Executive policies need to be formalized and funded by Congress before they can be enacted as national laws with a wide application. After much debate and compromise, Congress enacts legislation committing the resources necessary for the development of new cybersecurity policies, often adopting the executive branch's policies as its own. The executive branch then reinforces and executes Congress's mandate with further regulations and guidance. We will discuss Congress's role in the formation of cybersecurity laws in greater detail later in this chapter.

The Role of the Judiciary in Executive Policies

The judicial branch plays a narrow but critical role in cybersecurity law and policy, as federal courts hear and decide cases against individuals accused of violating the cybersecurity laws that Congress has passed and the president has signed. The courts also draft rules governing the type and length of punishment appropriate for individuals found guilty of violating these laws. We will discuss the judiciary's role in enforcing cybersecurity laws later in this chapter.

The Role of the Executive Branch

Article II of the U.S. Constitution states, "The executive Power shall be vested in a President of the United States of America." The president is the most powerful individual in the government; he is the commander-in-chief of the U.S. armed forces, the nation's chief diplomat, and the head of state. Within the U.S. federal government, only the president possesses the authority to issue executive orders and national security instruments. The president is also responsible for implementing and enforcing the laws created by Congress.

We have already discussed the president's role as "first responder" during national security emergencies. Following such emergencies, the president is the first to respond with policy decisions because, as a policymaker, he is more nimble than Congress; he can create new executive policies at any time. Conversely, congressional processes are more formalized and lengthy. Indeed, final decisions in Congress are usually the result of a long process of debate and compromise between rival parties.

Therefore, for the past 25 years, the executive branch has been the leader in developing U.S. cybersecurity policy. Executive policies identify priorities and direct resources toward particular agencies and programs.

For executive branch policies to have a wider effect beyond federal departments and agencies, they must be formalized and funded by Congress.

Structure of the Executive Branch

In practice, the executive branch is comprised of the president and the departments and agencies charged with enacting presidential policy. The president appoints the heads of these federal department and agencies. Some of these department and agency heads serve as members of the president's cabinet. Individually and collectively, federal departments and agencies and the cabinet are responsible for implementing, enforcing, and executing federal laws. Their missions, responsibilities, and priorities may evolve and change according to the orders of the president.

In 1939, Congress formed the **Executive Office of the President (EOP)** to assist the president and provide support for the increasingly large bureaucracy of the executive branch. The EOP consists of the following offices:

- The Council of Economic Advisers
- The Council on Environmental Quality
- The Executive Residence
- The National Security Council
- The Office of Administration
- The Office of Management and Budget
- The Office of National Drug Control Policy
- The Office of Science and Technology Policy
- The Office of the United States Trade Representative
- The Office of the Vice President
- The White House Office

The EOP plays an active role in the president's policymaking activities. Indeed, before a president finalizes an executive order or national security instrument, he participates in a deliberative process involving key departments and agencies of the EOP.

Key EOP Players: The National Security Council

The **National Security Council (NSC)** is a key agency in the development of cybersecurity policy in the executive branch. Created during the Truman administration and codified in the National Security Act of 1947, the NSC is the national security and foreign policy arm of the executive branch.

The NSC is comprised of the president, the vice president, the secretary of state, the secretary of defense, and the national security advisor. The president's chief of staff, the White House counsel, and the assistant to the president for economic policy are invited to attend NSC meetings. The chairman of the Joint Chiefs of Staff is the statutory military advisor, and the director of national intelligence serves as the intelligence advisor.

The NSC is instrumental in the creation of national security instruments, a type of presidential directive. These documents directly relate to national defense, foreign affairs, and national security—all areas that directly concern the NSC.

Key EOP Players: The Office of Management and Budget

Congress established the **OMB** (originally named the Bureau of the Budget) in 1921. The Bureau of the Budget became part of the EOP in 1939 and took on significant oversight responsibility for new government programs. Among its duties, the OMB determines and oversees the budget-making process of the federal departments and agencies.

During the administration of President Richard Nixon, the OMB acquired its current mission of managing and evaluating the programs of U.S. federal agencies and helping the president to create a federal budget according to its evaluations. Today, in addition to managing federal agencies and making budget plans for government programs, the OMB houses the federal government's Office of E-Government and Information Technology. This office works to streamline interactions between the government and the public using information technology, and it also works on cybersecurity initiatives.

The OMB's **Office of Information and Regulatory Affairs (OIRA)** works to reduce government paperwork and maintain an efficient flow of information within the government. As previously mentioned in Chapter 2, OIRA was formed after Congress passed the Paperwork Reduction Act of 1980. Because OIRA is charged with overseeing and implementing government-wide information policy, it is often involved in new federal computer-based initiatives. The websites of both the Office of E-Government and OIRA are good sources for policy documents related to federal computer and information security.

Key EOP Players: The Office of Science and Technology Policy

Congress established the **Office of Science and Technology Policy (OSTP)** as part of the EOP in 1976. The OSTP is charged with advising the president and his senior staff on matters related to science and technology. The scientific and technical expertise of the OSTP informs presidential policy and ensures that all new executive branch policies are based on scientifically sound information and analysis. The OSTP Resource Library is available to the public and contains important scientific speeches, documents, reports, testimony, policy guidance, and other potential research sources.

Key Types of EOP Policy Documents

Now that you understand the structure of the EOP, we will examine the most important types of policy documents and memoranda that the EOP produces. The EOP is a rich source of cybersecurity policy documents, many of which are accessible and form the basis of current federal laws, programs, institutions, departments and agencies, government positions, and regulations. Important new policies issued from the EOP may take the form of national security instruments, OMB memoranda, OSTP memoranda, executive orders, and White House strategy guides.

EOP Policy Document Type 1: National Security Instruments

A **national security instrument** is an often-classified order from the president to his cabinet ordering them to marshal resources around a policy. It lays out the intention and goals behind the policy and establishes a decision-making process involving specific government actors.

National security instruments concern national security policy and are therefore issued with the advice and consent of the NSC. Because of their national security significance, many national security instruments remain classified, even decades after they are issued. The fact that the EOP issued a national security instrument is public, but the content of that instrument may not be. National security instruments maintain their legal effectiveness indefinitely, even after the end of the issuing president's term, until a conflicting action is taken by a successor.

Generally, each administration has created a different name for its national security instruments, and recent presidents have used multiple names. For instance, President George W. Bush issued National Security Presidential Directives (NSPDs), while President Barack Obama issues Presidential Study Directives (PSDs), and Presidential Policy Directives (PPDs).[1]

National Security Instruments and Cybersecurity

Following the 1995 bombing of the Murrah Federal Building in Oklahoma City and the findings of President's Commission on Critical Infrastructure Protection (PCCIP), President Bill Clinton issued Presidential Decision Directive 63. PDD-63 established a structure under White House leadership to coordinate private-public sector sharing of threat and vulnerability information, in order to prevent physical and cyber attacks on critical infrastructure.

This historic directive was the first attempt to organize the government's response to an attack on critical infrastructure and to establish a critical infrastructure plan for cyber systems. PDD-63 formulated policies for national cybersecurity operations that have been reiterated in subsequent directives issued by Presidents Clinton, Bush, and Obama.

EOP Policy Document Type 2: Executive Orders

An **executive order (EO)** is a declaration from the president that is legally binding and does not require the consent of Congress. The president issues executive orders to federal departments and agencies. Many executive orders establish administrative procedures or powers. Like national security instruments, executive orders remain in place until a later president deliberately replaces them. Unlike national security instruments, executive orders are rarely classified.

Many executive orders concern national security and, increasingly, cybersecurity. For instance, in February 2013, President Obama issued **Executive Order 13636**, which called for new measures to enhance the cybersecurity of the nation's critical infrastructure. This EO highlighted cyber attacks as a major national security threat and encouraged the federal government to work with private sector entities to prevent cyber intrusions and enhance the protection of critical infrastructure. Specifically, the order emphasized the improvement of information-sharing as a key priority, calling upon the the federal government to "increase the volume, timeliness, and quality of cyber threat information" shared with the private sector.

Since the Oklahoma City bombing of 1995, presidents have issued many significant executive orders relevant to cybersecurity. As discussed in Chapter 2, President Clinton's Executive Order 13011 established the **Chief Information Officers Council (CIO Council)**. The CIO Council is comprised of CIOs from many federal

Video

Watch ‘Executive Order 13636’ at http://vimeo.com/channels/cybersecurityfoundations.

agencies. The CIO Council is the principal interagency group tasked with improving agency information resource management practices—including acquisition, design, development, use and sharing of information—in accordance with the Paperwork Reduction Act of 1980, the Government Performance and Results Act of 1993, the Information Technology Management Reform Act of 1996, the Government Paperwork Elimination Act of 1998, and the E-Government Act of 2002. In addition to creating the CIO Council, EO 13011 directed federal agencies to implement the provisions of the Paperwork Reduction Act and the Clinger-Cohen Act in order to improve the federal government’s management of information technology.

On October 8, 2001, less than one month after the 9/11 terrorist attacks, President Bush issued Executive Order 13228. This EO created the Office of Homeland Security and the Homeland Security Council as centers of the nation’s critical infrastructure protection. These bodies were the predecessors of DHS, which, as we will see in OMB Memorandum M-10-28, shares significant oversight powers for national cybersecurity with the OMB.

Executive Order 13231 created the position of special advisor to the president for cyberspace security. This position is also the head of the Office of Cybersecurity. EO 13231 also gave strategic responsibility for critical infrastructure protection to the executive branch by creating the President’s Critical Infrastructure Protection Board (PCIPB). The special advisor to the president for cyberspace security chaired the PCIPB and was responsible for recommending policies and programs to the EOP for protecting U.S. critical infrastructure.

A little more than two years after EO 13231’s release, the Bush administration announced another important policy document, referred to as Homeland Security Presidential Directive (HSPD) 7. Isssued in December 2003, HSPD-7 replaced PDD-63. HSPD-7 reiterated the administration’s commitment to partnership between lead government agencies and their counterparts in the private sector, and designated DHS as the lead agency for coordinating the nation’s overall critical infrastructure protection efforts.

Cyber Fact

Originally, the content of CNCI was classified, but in March 2010, in an effort to increase both the transparency and public awareness of CNCI, the Obama administration released high-level details about CNCI, in addition to publishing a Cyberspace Policy Review outlining the cyber threat environment and the cybersecurity priorities and strategies of the federal government.

Cyber Fact

“Initiative #1” of CNCI (“Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections”) reads as follows: “The Trusted Internet Connections (TIC) initiative, headed by [OMB] and [DHS] proposes the consolidation of the Federal Government’s external access points (including those to the Internet). This consolidation will result in a common security solution which includes: facilitating the reduction of external access points, establishing baseline security capabilities; and, validating agency adherence to those security capabilities.”

In 2008, the Bush administration issued NSPD-54/HSPD-23, which launched CNCI. With CNCI, President Bush elevated the issue of cybersecurity to a new level of national importance, involving DHS, the OMB, and the NSA. President Bush's CNCI also identified national cybersecurity priorities for the federal government.

Federal departments and agencies are assigned the responsibility of executing initiatives outlined in CNCI and reporting back to the EOP. The goal is for these initiatives to become part of the day-to-day cyber operations of the White House and the federal government.

EOP Policy Document Type 3: OMB Memoranda

OMB memoranda are important policy documents that can shed light on how power over the government's cybersecurity operations can shift at the OMB's discretion. The director of the OMB has issued nationally significant memoranda about cybersecurity, including FISMA reporting requirements for federal departments and agencies. These memoranda clarify the specific responsibilities of departments and agencies with regard to national cybersecurity policy.

An important OMB memorandum for cybersecurity researchers to examine is M-10-28. In this memorandum, the OMB gave DHS "primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA [...]" In other words, M-10-28 gave DHS the responsibility to oversee the cybersecurity programs of all federal departments and agencies, with the stipulation that DHS report to the OMB. In turn, the OMB reports directly to the president on the effectiveness and cost-efficiency of these cybersecurity programs. Therefore, this document is the basis for the current federal power structure for enforcing FISMA.

M-10-28 also solidified the role of the cybersecurity coordinator, a position created by President Obama in 2009 (see Chapter 2). The OMB acknowledged the coordinator's lead role in interagency cybersecurity initiatives, and formally tasked the coordinator with working with DHS to oversee FISMA compliance and "[coordinating] interagency cooperation with DHS cybersecurity efforts."

Cyber Fact

The **Federal Information Security Management Act of 2002 (FISMA)** requires all federal departments and agencies to develop and implement robust information security programs on a budget, and to report to the OMB.

EOP Policy Document Type 4: OSTP Memoranda

Another EOP office that issues memoranda related to cybersecurity policy is the OSTP. On December 17, 2010, the OSTP issued a memorandum called **"Scientific Integrity."** This memorandum lays out several principles of importance to the OSTP, including the idea that "[I]t is important that policymakers involve science and technology experts where appropriate and that scientific and technological information and processes relied upon in policymaking be of the highest integrity." OSTP's "Scientific Integrity" memorandum also advocates that government agencies foster open communication between scientific experts, hire spokespeople to articulate scientific work in a nonpartisan fashion, and ensure "[t]he accurate presentation of scientific and technological information" for policymakers and the public.

This memorandum notes that the director of the OMB will issue guidance to OMB staff regarding standards to be upheld in the review of executive branch testimony on scientific issues. It concludes by asking that agencies report back to the OSTP on steps they have taken to improve the scientific integrity of their work and presentations. Although this OSTP memorandum did not create any new rule or reassign power, it is a document that both affects and reflects policymaking at the executive level.

EOP Policy Document Type 5: White House Strategy and Guidance

The White House and federal departments and agencies issue annual reports that inform, guide, and reflect executive policy on cybersecurity. The 2010 Quadrennial Homeland Security Review report and the 2010 Bottom-Up Review report identified cybersecurity as a key mission area for DHS. The 2011 Blueprint for a Secure Cyber Future and the 2012 DHS Strategic Plan set forth a clear strategy for forming private-public partnerships around cybersecurity. These documents, as well as other cybersecurity publications, offer more details than executive orders or PDDs because they deal with specific plans rather than broad policies and executive priorities. Students of cybersecurity should also review the Obama administration's 2009 Cyberspace Policy Review and 2011 International Strategy for Cyberspace. Both of these documents discuss current policy objectives and obstacles for federal cybersecurity.

Executive Branch Research Source: The Federal Register

Certain types of presidential directives are published in the ***Federal Register.*** The *Federal Register* is a daily publication of the U.S. federal government, created in 1935. According to the official website of the National Archives, each issue of the *Federal Register* is organized around four categories: (1) "Presidential Documents" ("including executive orders and proclamations"); (2) "Rules and Regulations" ("including policy statements and interpretations"); (3) "Proposed Rules" ("including petitions for rulemaking and other advance proposals"); and (4) "Advance Notices" ("including scheduled hearings and meetings open the public, grant applications, and administrative orders"). The simplest way to search for information in the *Federal Register* is online.[2]

The Role of the Legislature

The purpose of this section is to explain how Congress develops and enacts cybersecurity legislation. As previously discussed, when catastrophic events occur, the executive branch is usually the first branch of the federal government to respond, because Congress must go through a formal process of proposing, drafting, debating, and voting on legislation. Executive response may take the form of legally binding executive orders or national security instruments; however, Congress is the only authority that can fund the programs created by executive policies.

Congressional Authorities

Article I of the U.S. Constitution states, "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives." Congress is a bicameral body consisting of the House of Representatives and the Senate. Each state in the U.S. elects two senators. Each state also elects representatives to the House, the number of representatives being proportional to each state's population.

Congress's primary authority is its control of the federal government's ability to fund new and existing programs; that is, it holds the "power of the purse." Congress also has the authority to create new federal departments and agencies, and to reorganize existing ones. For instance, in 2002, Congress created the DHS pursuant to its passage of the Homeland Security Act (HSA). The reorganization of federal departments and agencies following the passage the HSA was the largest federal government reorganization since the NSC was established in 1947.

The Homeland Security Act as a Model for Modern National Security Legislation

Congress has typically followed the president's lead on cybersecurity policy. Through Congress, presidential priorities become legal requirements that form the basis of government programs.

As discussed earlier in this chapter and in Chapter 2, President Clinton's PDD-63 is an historic cybersecurity policy document. Indeed, Congress incorporated many of its elements into the HSA. For example, PDD-63 created the **National Infrastructure Protection Center (NIPC)**. This organization is charged with protecting critical infrastructure, with special attention paid to computer systems. The NIPC sends out alerts and warnings regarding new threats and vulnerabilities. Formerly housed within the FBI, the NIPC was codified in the HSA and has been operated by DHS since the latter was formed in 2003.

Thus, the HSA was an important piece of cybersecurity legislation that affected cybersecurity policymaking and operations by creating new offices, programs, and positions dedicated to cybersecurity. It also rearranged and reassigned responsibility among existing departments and agencies. It was a landmark piece of legislation for cybersecurity policymaking at the federal level.

How Congress Passes Bills into Laws

Typically, a legislator (a representative or senator) introduces a bill for consideration. A **bill** is a proposed piece of legislation.

Bills typically originate in the House of Representatives, though they may also originate in the Senate. House members may introduce a bill at any time, and in any way, while Congress is in session. For example, a House member may make a speech about why he is introducing the bill, or he may simply place a written statement in a wooden box called "the hopper," located in the House chamber. A proposed bill is assigned a number (e.g., H.R. 1 for a bill that originates in the House, or S. 1 for a bill that originates in the Senate) and clearly states the name of its sponsor—the member of Congress who wrote it. Bills may also be co-sponsored.

The Speaker of the House passes proposed bills along to the appropriate congressional committees. **Committees** are congressional groups focused on a specific national issue. There are congressional committees on nearly every subject matter, including the budget, finance, and foreign relations. A great deal of congressional work happens in committees, and committees decide which bills will be voted on by the entire House or Senate. Several committees are charged with reviewing each proposed bill.

Discussions of bills begin with closed-door talks between committee members and representatives from the relevant government departments and agencies. These department and agency representatives offer their input before a committee deems the bill to be of sufficient importance to call for public hearings. At public hearings, members of the public may testify before members of Congress on the desirability or importance of passing a given bill and enacting it into law.

Following the public-hearings stage of the legislative process, a congressional committee will consider the bill again in a period known as the mark-up session. During the **mark-up session**, a committee or special subcommittee studies the proposed bill in depth and from both sides of the issue. The members of the committee or subcommittee consider the input and testimony they have received from the departments and agencies, from the public, from advocacy groups and lobbyists, and from experts. They then decide whether or not to recommend the bill and whether or not to amend the bill before recommending it.

At the end of the mark-up session, and after receiving the recommendations of any relevant subcommittee, the full committee votes on whether or not to recommend the bill to the full House of Representatives (or to the Senate, if that is where the bill originated). If the committee does recommend the bill, they must vote on whether or not, and how, to amend the proposed legislation before recommending it. The committee may ultimately decide not to recommend the bill, or to postpone the committee vote indefinitely.

Should the committee vote in favor of recommending the bill to the full House of Representatives (or Senate), it will draft a committee report explaining its reasons for recommendation and, if applicable, explaining any amendments added to the bill. The committee will generally address each section of the bill and explain in detail what each section is meant to accomplish as part of a proposed new law. In order to justify congressional funding, the report must include a proposed budget and a statement of objectives and outcomes. Each committee report must also include a statement that cites the constitutional powers granted to Congress that allow Congress to pass this specific bill into law.

When a bill is recommended by all of the committees in which it was examined, Congress places it on the legislative calendar for floor debates. The **floor** is the term for the conceptual place in which all official activity in Congress happens. During floor debates, the proposed bill is read at least twice on the floor of the House. The second time the bill is read, representatives may propose amendments to each section.

Following floor debates in the House, the representatives take a final vote on whether or not to send the bill to the Senate (or, if the bill originated in the Senate, whether or not to send the bill to the House). Voting in the House may be conducted in several ways: (1) *viva voce*, in which representatives voice their vote aloud; (2) through a method known as *division*, in which representatives vote for or against a bill by standing up; or (3) using an electronic voting system. A majority vote means that the bill has passed the House and will be delivered to the Senate for another vote. The content of the proceedings and debates that take place on the floors of both the House of Representatives and the Senate are published in the ***Congressional Record***, a report issued daily when Congress is in session.

A bill that passes in the House of Representatives and is sent to the Senate (or passes in the Senate and is sent to the House) becomes an *act*. An act goes through a similar legislative process in the Senate, with senators debating the its merits on the floor and proposing new amendments. Voting in the Senate is *viva voce* and a majority vote is needed for the act to pass.

If an act passes, but a similar but conflicting piece of proposed legislation has previously been passed in the Senate (for bills originating in the House), a conference committee may be assembled to reconcile differences between the two pieces of legislation before the final legislation is delivered to the president. **Conference committees** are composed of members of both the House and the Senate and are considered especially critical for reconciling legislative differences on bills that are controversial in nature.

A bill that has passed in both the House and the Senate is finally sent to the president for signature. The president has 10 days to publicly approve the bill (by signing it) or to publicly disapprove of it by exercising his **veto power**. The Constitution grants the president this veto power, which allows him to return a proposed bill to the part of Congress (either the House or the Senate) in which it originated. When the president vetoes a bill, he usually adds an explanation of his reasons for vetoing it. The president's veto can be overridden by a two-thirds majority vote in both the House and the Senate. Bills that the president neither signs nor vetoes automatically pass into law after 10 days. All bills that pass both the House and Senate and are either signed by the president or not vetoed become public laws that the federal government must enforce.

Where To Find Proposed Bills and Laws

Congress's website offers the complete texts of bills and laws, along with easy access to the *Congressional Record* and other information about Congress

Another fantastic tool for accessing legislation and its history is **THOMAS.gov**, a service provided by the Library of Congress, the federal government's research library. THOMAS, named after Thomas Jefferson, is an exhaustive database of congressional and presidential activity and documents, and allows researchers to search for past and proposed legislation.[3]

Research Source: the Government Accountability Office

The **Government Accountability Office**, previously referred to as the General Accounting Office, is a nonpartisan agency that works for Congress and is charged with making Congress better informed, more efficient, more ethical, and more responsive. The GAO's duties include investigating how taxpayer dollars are spent and auditing the activities and performance of federal departments and agencies. The GAO also assists Congress in conducting audits, investigations, and evaluations. For this reason, the GAO is sometimes referred to as Congress's "watchdog." In addition to these research and investigative activities, the GAO's Office of General Counsel makes legal decisions and submits legal opinions.

The GAO's website is a rich source of cybersecurity research materials. Recent GAO reports and testimonies, as well as legal decisions, are available on this website, and one can search by topic, agency name, or agency type. In addition, the website has a section to help researchers perform more effective searches.[4]

Research Source: Congressional Research Service

The **Congressional Research Service (CRS)** is another legislative branch research and information agency. The CRS is housed in the Library of Congress and works exclusively to perform policy and legal analysis for Congress. The CRS employs over five hundred researchers—policy analysts, attorneys, and experts—and has been nicknamed "Congress's Think Tank."

The mission of the CRS is to provide comprehensive, objective research to members of Congress, and to contribute to informed debate in the national legislature. Therefore, CRS performs research at every step in the legislative process. Its researchers examine all sides of an issue, research specific questions for members of Congress, and provide policy alternatives. CRS research provides members of Congress with analytical information in the topic areas of "American Law," "Domestic Social Policy," "Foreign Affairs, Defense, and Trade," "Government and Finance," and "Resources, Science, and Industry."

Congress controls the distribution of all CRS research, and CRS research remains confidential except in special cases in which Congress authorizes its release. Individual researchers may request access to these specific CRS documents. While these requests are usually declined, individual members of Congress may choose to provide some of the research to researchers who call. Requests for access to CRS research have a better chance of being approved if the researcher can, in turn, assist CRS with its work—for example, if a researcher can contribute an expert opinion to a CRS research project.

Federal Regulations: The Executive Branch and the Legislative Branch Combined

The purpose of this section is to discuss how and why federal regulations are created. A **regulation** is an enforceable law that has been authorized by congressional legislation or an executive order to remedy a specific problem. A regulation may create boundaries or limitations, establish a duty, or assign accountability to an industry, sector, or organization.

Some regulations attempt to exert a degree of control on the economy. Minimum wage laws are an example of this type of regulation. Some regulations focus on public health and safety, such as the regulation that requires all cars to carry seatbelts for passengers. In general, regulations attempt to promote certain kinds of outcomes by imposing restrictions, requirements, or incentives that favor those outcomes. Of course, new federal regulations must be legally justified and authorized by Congress and the president.

Some federal agencies are referred to as **"regulatory agencies"** because issuing regulations is one of their primary activities. The Food and Drug Administration (FDA), a federal agency within the Department of Health and Human Services, is one example of a regulatory agency. The FDA issues specific regulations about food and drugs; for example, the FDA regulates which drugs may be legally manufactured and sold in the United States. The FDA's authority to create these regulations stems directly from a specific piece of congressional legislation: the Food, Drug, and Cosmetic Act of 1938. This act increased the federal government's power to regulate these potentially hazardous products.

Congress (through legislation) or the president (through an executive order) can create an agency and grant it the authority to regulate certain sectors or industries. For a review on the process of how Congress directs a department or agency to fulfill an objective, see Chapter 3. A regulatory agency may decide to issue a new rule on its own. However, this regulation cannot exceed the agency's statutory authority, and the agency must have an open public discussion as required by the **Administrative Procedure Act (APA)** of 1946. As its name implies, this act established the procedures by which federal departments and agencies may propose and enact new regulations.

The Regulation-Making Process: From Advance Notice to Final Rule

At the beginning of the rulemaking process, the regulating agency may publish an **advance notice of proposed rulemaking (ANPR)** in the *Federal Register*. An ANPR is a formal invitation for the public to participate in shaping a proposed regulation. By law, federal agencies are required to keep the public informed about all new proposed regulations, and the *Federal Register* is the forum through which federal agencies communicate proposed regulations to the public.

Following the ANPR, the agency publishes a proposed rule in the *Federal Register*. The **proposed rule** announces and explains the agency's plan to address a problem or accomplish a goal. It begins with a summary section—a brief discussion of the rule and why the agency deems it necessary, along with an explanation of the

VIDEO

Watch 'Regulations Research Tutorial' at http://vimeo.com/channels/cybersecurityfoundations agency's legal authority to create the rule—followed by an invitation and deadline for public comments. In 1998, an official electronic comment portal was created for the public to participate in the creation of federal regulation.

The **notice and comment period** is the time during which the agency is required to gather input from experts and the general public. Most agencies are legally required to respond to all public comments submitted during the notice and comment period. Agencies may hold public hearings during this period. The notice and comment process allows the agency to evaluate its proposed rule based on the comments, scientific data, and expert opinions it accumulates during this time. Agencies may consider comments submitted after the official close of this process, even though they are not legally bound to do so.

At the end of this process, the agency considering the new rule must conclude that its proposed regulation will help it to accomplish its specified goal or solve its particular problem. The agency must also consider alternative solutions that would be more effective or cost less. Typically, the notice and comment period will be followed by either a new and substantively amended proposed rule or by a **final rule**. The final rule will have an **effective date**. This is the date at which the rule becomes enforceable. The *supplemental information* section that accompanies the final rule sets out the goal or problems that the new rule addresses, describes the facts and data the agency relied on in its rulemaking process, responds to major criticisms made during the notice and comment process, and explains why the agency did not choose alternative rules.

An agency may publish a final rule without a proposed rule in limited cases where the agency has "good cause" to find that the notice and comment process would be impracticable, unnecessary, or contrary to the public interest. These cases may be emergencies in which public health is at risk, cases in which Congress has already directed a specific regulatory outcome by law, or cases of minor technical amendments. An agency gives the label "interim final rule" to a final rule that it has created without first asking for public comment on a proposed rule. An **interm final rule** is effective immediately, and the agency may modify it based on public comments after it goes into effect. After the final rule is published, the regulating agency may publish guidance material, so that individuals and industries will better understand the new regulatory requirements.

Legislative and Judicial Roles in Regulations

By law, agencies must send final rules to Congress and the GAO before these new regulations can take effect. Congress may pass a resolution of disapproval on the regulation, which, if signed by the president, renders the regulation void. A president may also exercise his veto power on a new regulation, though Congress may overrule this veto with a two-thirds majority.

The judicial branch is also involved in the process of enacting new federal regulations. A court may rule that a regulation is unconstitutional, goes beyond the agency's legal authority, was made without following the notice and comment process required by the APA, or was an abuse of the agency's discretion. The rule is then sent back to the agency, and the agency, which can reopen the comment period or correct the legal problems identified by the court.

The Code of Federal Regulations

Federal department and agency rules and regulations are published online in the ***Code of Federal Regulations* (CFR)**. The CFR provides a complete listing of federal regulations, organized by year and policy title. The CFR is published annually.[5]

The Role of the Judiciary

The purpose of this section is to discuss the role of the judicial branch in cybersecurity law and policy. The **judicial branch** is the federal legal system, or "the courts." Judiciary powers are granted in Article III of the U.S. Constitution. Article III establishes the Supreme Court of the United States and gives Congress the power to establish lower courts. Article III, Section 1, of the Constitution reads, "The judicial power of the United States, shall be vested in one Supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish". **Inferior courts** refer to the district and appeals courts, collectively known as the *federal court system*.

The district courts are the trial courts of the nation. There are a total of 94 federal districts that decide criminal and civil cases. Of the 94 federal district courts, there are 12 regional circuits—known as the Court of Appeals. The Court of Appeals listens to the appeals from the district courts.

Cyber Fact

An **appeal** is a request made after a trial by a party that has lost on one or more issues; a higher court reviews the original decision to determine if it was correct. To make such a request is **"to appeal."** One who appeals is called the **"appellant,"** while the other party is referred to as the **"appellee."**

While the Constitution does not mention laws or measures concerning information security, or even suggest such measures, the broad language of the document gives federal courts the authority to make legal rulings that affect national cybersecurity law and policy. Still, in comparison to the executive and legislative branches, the judiciary's role in cybersecurity policy is limited. Traditionally, the judiciary's role in cybersecurity has been to enforce the federal laws that Congress has enacted to deter cyber crime.

Thus, the judicial branch of the federal government is the venue for the prosecution of accused cyber criminals. The judicial branch also determines sentencing for cyber criminals found guilty in court. Finally, the judicial branch and the federal courts play an important role by adding a voice to the theoretical debates around cybersecurity. As we will see when we examine case studies in depth, court rulings may contribute to philosophical arguments about cybersecurity issues, such as the ongoing struggle between the privacy and security communities, or the question of which entities are ultimately responsible for cybersecurity failures.

To offer just one example, in *United States v. Jones*, the Supreme Court upheld the Court of Appeals' ruling, which reaffirmed privacy rights with regard to new technology. In the case under examination, a man

Cyber Fact

One important aspect of the way the judicial system works is the idea that decisions in important cases are informed by decisions in cases that came before: this is the idea of **judicial precedent**. Because cyber crime is a relatively new field for judicial decisions, the role of the courts will continue to evolve as more cyber crimes are prosecuted in the years and decades to come. Future court decisions, and what these decisions show about the adequacy or inadequacy of existing cyber laws, may influence the development of new laws in Congress.

was charged with drug trafficking after the police placed a GPS tracking device on his wife's car. The Supreme Court ruled that this action, undertaken without a warrant, infringed upon the man's Fourth Amendment right against unreasonable search and seizure.[6] This case set the current precedent regarding limitations on the use of surveillance technology in law enforcement.

Most cyber crimes are prosecuted as federal crimes rather than state crimes because the jurisdictions (scope of authority) of many state courts do not yet cover cyber crimes. Therefore, individuals accused of committing cyber crimes will likely find themselves tried in the federal criminal court system.

Congress has passed several pieces of legislation regarding cyber crime. This legislation makes it illegal to damage or steal information from computers. Among the laws dealing with cyber crime are the **Computer Fraud and Abuse Act** (1984), the **Electronic Communications Privacy Act** (1986), and the **Identity Theft Penalty Enhancement Act** (2004). Together, these statutes form a comprehensive legal strategy to deter and punish hackers. All three acts escalate sentences and fines based on the severity, sophistication, and magnitude of the offense. A detailed explanation of each act follows.

Cyber Law Example 1: The Computer Fraud and Abuse Act (CFAA)

In order to give the judiciary the authority to both try and convict hackers who commit cyber crimes, Congress passed the Computer Fraud and Abuse Act (CFAA) in 1984. Since its passage, the CFAA has been amended several times to improve its effectiveness and to criminalize new threats.

The first person to be convicted under the Computer Fraud and Abuse Act was Robert Morris, the author of the "Morris worm." The Morris worm was the infamous first computer worm, a malicious software program designed to spread from computer to computer (for more information on computer attacks and exploits, see Chapter 4. For more on the Morris worm specifically, see the Introduction to this book). Robert Morris claimed that, when he created the Morris worm, his intent was not to commit harm but only to determine the size of the Internet. Despite his claim of innocence, the worm caused significant damage to private and public-sector networks. Following multiple appeals, Morris was sentenced to three years of probation, four hundred hours of community service, and a $10,000 fine.

The seven types of criminal activity prohibited by the CFAA are listed below.[7]

Obtaining National Security Information

Disclosing or attempting to disclose classified information, acquired by unauthorized network access, relating to national defense, foreign relations, or atomic energy, with reason to believe the actions could injure the United States or be used to the advantage of foreign nations. The statutory penalty is not more than ten years (not more than twenty years for repeat offenders).

Accessing a Computer and Obtaining Information

Acquiring protected information through gaining unauthorized access to government computers, computers belonging to financial institutions, or computers involved in interstate commerce. Statutory penalties begin at less than one year. For crimes involving more than $5,000, penalties are elevated to five years or less. Repeat offenders may receive ten years or less.

Trespassing in a Government Computer

Hacking into federal government computers (computers used exclusively or in part by the federal government). Offenders can be imprisoned for not more than one year, or not more than ten years if they are a repeat offender.

Accessing a Computer to Defraud or Obtain Value

Essentially, hacking into a government computer, financial institution computer, or any computer involved in interstate or foreign commerce (a very broad standard which arguably could apply to the majority of computers), with intent to defraud. Committing computer fraud may include stealing financial information or other confidential information that could be used to perpetrate identity theft. This section carries a statutory penalty that cannot exceed five years, or in the cases of repeat offenders, ten years.

Causing Computer Damage

Unleashing worms or viruses, or other actions that cause damage to government computers, financial institution computers, or computers used in interstate commerce. Statutory penalties range from up to one year for negligent conduct, up to five years for reckless conduct, and up to ten years for intentional conduct. Repeat offenders may receive up to ten years for negligent conduct and up to twenty years for reckless or intentional conduct.

Trafficking Password Information

Trafficking in computer passwords or other computer keys with the intent to defraud. If a person steals a password in order to enter a government system, he or she violates this section. The statutory penalty is up to one year and up to ten years for repeat offenders.

Extortion Involving Computers

Any threat to cause damage to a protected computer (a government computer, financial institution network, or computer involved in interstate commerce) with the intent to extort money. The statutory penalty is not more than five years and not more than ten years for repeat offenders.

Recent amendments of the CFAA significantly broadened the definition of a "protected computer" – that is, a computer protected under terms of the CFAA. Under the CFAA, any computer that affects interstate commerce is considered to be a "protected computer." This inclusive terminology encompasses computers that are connected to the Internet, computers that are not connected to the Internet, and even computers located outside of the United States. The inclusive nature of the CFAA makes this statute the most comprehensive cyber crime law to date, and the statute that courts most often rely upon to convict hackers.

Case Study: Albert Gonzalez and the CFAA

In 2009, one of the country's most infamous hackers was found guilty of violating the CFAA. Albert Gonzalez was charged with orchestrating cyber attacks on TJX and Heartland Payment Systems. These attacks allowed Gonzalez and his team to steal hundreds of millions of credit and debit card numbers and resulted in tens of millions of dollars in fraudulent charges. Gonzalez was indicted and pled guilty to violating the CFAA. He was sentenced to two concurrent twenty-year terms in federal prison for his crimes. For more information on this case, see Chapter 5.

Cyber Law Example 2: The Electronic Communications Privacy Act and the Wiretap Act

Federal prosecutors may charge hackers with violation of the Electronic Communications Privacy Act (ECPA), in addition to violation of the CFAA. Specifically, the section of the ECPA called the **Wiretap Act** makes it illegal to intercept or disclose illegally intercepted wire, oral, and electronic communications without a search warrant. Spyware, packet sniffers, or any other information collection software that intentionally attempts to intercept electronic communication is prohibited by the Wiretap Act. Penalties under this act include imprisonment for up to five years and fines of up to $250,000 for individuals.

Cyber Law Example 3: The Identity Theft Penalty Enhancement Act

As discussed in Chapter 4, many cyber attacks are motivated by the attacker's desire to obtain personally identifying information—including names, bank account numbers, credit card numbers, and Social Security numbers that can be used to steal a victim's identity. Identity theft is often the result of cyber data breaches.

The Identity Theft Penalty Enhancement Act of 2004 established a new crime: aggravated identity theft against U.S. citizens. The act established two offenses, one that includes general identity theft crimes and another that is a terrorism offense. With regard to the general offense, the act declares that, "Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years." Meanwhile, with regard to the terrorism offense, the act declares that "Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years." Additionally, restitution to the victims may be ordered "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm" caused by the offense.

The Federal Criminal Procedure Process

In a federal criminal case, a **U.S. attorney** is the prosecutor. Each U.S. attorney is a member of the executive branch, and his or her job is to enforce federal law by prosecuting accused federal criminals in U.S. federal courts.

The **grand jury** is a jury, composed of between 12 and 23 citizens, that reviews evidence presented by the U.S. attorney and determines whether or not there is **probable cause** for a criminal charge—known facts leading to a reasonable belief that a crime was committed—that would lead one to believe that an individual has committed a crime. If a majority of the grand jury decides there is sufficient evidence to constitute probable cause, it will issue an **indictment**—a formal accusation. The indictment charges the individual with a violation of the law and gives the FBI and law enforcement officials the authority to arrest the accused individual.

After the individual is charged a violation of a cyber crime statute, he is arrested and a date is set for him to appear before a federal judge. The judge determines whether the defendant should be held in jail until trial or whether he is eligible for bail. If he is eligible for bail, the defendant may deposit funds with the court in exchange for his temporary release, upon the condition that he returns for his trial. At the arraignment, the defendant enters a plea to the charges brought against him. An agreement in which the defendant pleads guilty in return for the U.S. attorney agreeing to drop certain charges or recommend a lenient sentence is called a **plea bargain**. If the defendant pleads not guilty, the judge will proceed to schedule a trial.

In a federal criminal trial, the burden of proof is on the U.S. attorney, who must prove to the jury that the defendant committed the crime **"beyond a reasonable doubt."** This standard means that the evidence against the defendant must be so strong that there remains no reasonable doubt that the defendant committed the crime. The trial jury (composed of 12 citizens, usually selected from the same general pool as the case's grand jury) must vote unanimously that the defendant is guilty in order for him to be found guilty by the court and sentenced.

If the jury returns a verdict of "guilty," the judge will determine the defendant's sentence (statement of punishment) based on: (1) the penalties outlined in the statute and (2) the Federal Sentencing Guidelines. The ***Federal Sentencing Guidelines*** are issued by the United States Sentencing Commission and determine the length of a convicted criminal's jail time based on a point system.

Cyber Fact

The **United States Sentencing Commission (USSC)** is an independent agency in the judicial branch of government. Its principal purposes are: "(1) to establish sentencing policies and practices for the federal courts, including guidelines to be consulted regarding the appropriate form and severity of punishment for offenders convicted of federal crimes; (2) to advise and assist Congress and the Executive branch in the development of effective and efficient crime policy; and (3) to collect, analyze, research, and distribute a broad array of information on federal crime and sentencing issues, serving as an information resource for Congress, the Executive branch, the courts, criminal justice practitioners, the academic community, and the public."[8] The USSC created a point system that assigns an offense value to crimes. Under this system, a judge assigns a crime an offense value between 1 and 43 points. The more serious the court determines the crime to be, the higher the point value a judge will assign. The point value assigned to a crime helps to determine the criminal's sentence. A crime assigned just 1 point calls for a prison sentence of 0-6 months, while the highest offense level, 43, calls for life imprisonment.

Once the base value is determined for a cyber crime, the judge may add additional points based on a number of factors related to the specific cyber crime, including whether or not it involved a computer used for U.S. national security or defense purposes, and whether or not the conduct disrupted or damaged critical infrastructure. The base offense level for violations against the CFAA ranges between 6 and 35. The base offense level may be increased according to the amount of the victim's monetary loss (which the prosecutor has the burden of proving), the number of victims that suffered a loss as a result of the offense, and where the offense originated. Furthermore, the judge may add additional points if the offense involved "sophisticated means," or tactics that increased the risk of death or serious bodily injury for the victims, or are related to critical infrastructure.

In 2011, the Obama administration called for increased penalties to deter and disrupt the growing number of data breaches and denial of service attacks on the private and public sectors.[9] Administration officials contended the severity of the punishments was not proportional to the seriousness or complexity of the crime and called for increased prison sentences and fines under the CFAA. It is likely that new laws and harsher sentencing guidelines will arise as the number and capabilities of cyber criminals continue to increase.

Cybersecurity: A Global Perspective

The Internet does not belong to any nation or state. This "network of networks" is a global asset involving global management, global risks, and global responsibilities. Cyber crime, cyber espionage, and cyber warfare

Cyber Fact

A Brief History of International Cyber Attacks

Chechnya, 1990s : Chechen guerilla propaganda and fund-raising websites impact public perception of the Russo-Chechen conflict. The Russian government hacks into these websites and changes their content.

Kosovo, 1999: During the Kosovo war, the pro-Serbian hacker group known as the "Black Hand" targets the U.S. Navy and NATO with virus-infected emails in a DoS attack. The White House website is disrupted, and the NATO Public Affairs website is taken down.

China, 2001: U.S. and Chinese "patriotic hacker" activity flares after the downing of a US Navy EP-3 aircraft. The FBI warns U.S. businesses of "malicious" Chinese hacker activity and investigates a possible compromise of California's electric power grid. In 2002, the Chinese government calls off anniversary attacks, suggesting that Chinese hackers respond to government command and control.

Estonia, 2007: Following Estonian relocation of a Soviet war monument, pro-Russian hackers supplement rioting on the streets by successfully compromising Estonian government, media, and banking websites for three weeks.

Syria, 2007: A cyber attack reportedly deactivates a Syrian air defense system prior to the Israeli Air Force's destruction of an alleged nuclear reactor.

United States, 2010: In January 2010, Google reports that an advanced persistent threat attack originating in China, later dubbed "Operation Aurora," has been carried out against Google and dozens of other organizations for at least six months.

Iran, 2010: The Stuxnet computer worm destroys an estimated 1,000 Iranian nuclear centrifuges.[10]

United States, 2011: A computer virus infects networks at the U.S. drone fleet control center in Nevada. Not long after, Iran captures a U.S. military drone, claiming it commandeered the craft's control systems via cyber attack.

are relatively new phenomena, but they are all growing quickly in volume and sophistication. As these threats and tactics evolve, they will present law enforcement, national security planners, and corporate directors across the globe with challenges of increasing magnitude and consequence. Examples of some recent international cyber attacks can be found on the following page.

One area of intense research focus over the last ten years concerns the connection between computer networks and national critical infrastructure. Information systems from telecommunications to banking to power grids are increasingly dependent on the Internet for basic operations. In both the private sector and the public sector, this increased dependence on the Internet implies increased vulnerability to cyber attacks, cyber espionage, and other kinds of cyber crime.

World events, primarily the 2007 attacks in Estonia and the 2010 Stuxnet worm, have defined the formative years of cyberspace warfare. The 2010 Stuxnet worm, which destroyed as many as 1,000 nuclear centrifuges in Iran, has already proven that a malicious computer code can inflict physical damage on industrial infrastructure. In 2012, it was revealed that the United States has continued to use the Stuxnet worm to launch attacks on Iran's nuclear facilities. The U.S. is also suspected to be playing a key role in developing the newer and more complex Flame malware to conduct cyber espionage against its adversaries. In April 2012, a Flame cyber attack against Iran forced the country's Oil Ministry to disconnect its computers from the Internet in an attempt to defend itself from the virus.

Cyber Fact

Events in the physical world are now mirrored in cyber space. For example, during the 2008 South Ossetia War, concurrent cyber attacks were launched between Russia, Georgia, South Ossetia, and Azerbaijan. These attacks resulted in the defacement of the Georgian parliament's website, as well as the hacking of South Ossetia's primary news website and radio station. Similarly, cyber weapons are prevalent in the ongoing Iran-Israel shadow wars and in the growing military and political tension between the U.S. and China.

While there have been limited verifiable accounts of cyber attacks on critical infrastructure so far, many analysts believe that first-tier militaries and intelligence agencies have sufficient knowledge of both hacking and critical infrastructure functions to conduct such attacks. National risk managers categorize this kind of cyber attacker as an "advanced persistent threat" (APT).

IANA, ICANN, and IETF: Coordinators of the International Internet

In the early days of the Internet, engineers created a global IP address registry, a list of IP addresses, and the details of the organizations that corresponded to these addresses. The **Internet Assigned Numbers Authority (IANA)** was founded by the U.S. government in 1988 to manage global IP address assignments. IANA was quickly overwhelmed as more and more organizations joined the Internet. IANA now operates as a department of the **Internet Corporation for Assigned Names and Numbers (ICANN)**

In 1998, with the encouragement of the U.S. government, ICANN was created both to coordinate the assignment of IP addresses and to keep the Internet running smoothly and securely in the era of its unprecedented and growing popularity. In particular, ICANN would manage the Internet's Domain Name System as it grew with the World Wide Web and became increasingly international. Management and coordination of the DNS ensures that every address is unique and that all valid addresses can be found by all Internet users.

Today, ICANN coordinates the DNS, IP addresses, protocol identifier assignment, and root server system management functions, among other tasks. These tasks were originally performed by the IANA. It is important to note that ICANN has no responsibility for any of the content or activities on the Internet. Its role is simply to organize the Internet according to protocols.

ICANN's core purpose is to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet. Within the context of its mission related to the Internet's unique identifiers, ICANN plays an active role, contributing to global efforts to address security, stability, and resiliency challenges faced by the Internet.

Cyber Fact

On a traditional map, we are used to seeing state and town names instead of a technical number, such as a GPS coordinate or measurements of longitude and latitude. The same principle applies on the Internet—instead of complicated IP addresses (e.g., "232.44.12.13"), we use easy-to-remember names (e.g., "www.mydomain.com"). These user-friendly names are automatically translated for Internet users by the DNS, which function as a kind of Internet phone book.

ICANN functions a non-profit organization that encourages the participation of the public and aims to be transparent in its operations. ICANN views the public sector, the private sector, and technical experts as peers, and seeks input from hundreds of communities of users. ICANN operates under the belief that all users of the Internet deserve a say in how this global resource is managed.

In 2006, ICANN entered into an agreement with the U.S. Department of Commerce. The agreement emphasized the security of the Internet as a primary concern and articulated the joint goal of eventually moving DNS management to the private sector. For cybersecurity researchers, ICANN's website is an excellent source of information and official documents about how the Internet is managed.

In 1992, the **Internet Engineering Task Force (IETF)** recommended the establishment of subsidiary organizations to allocate and manage IP addresses for specific regions of the world. These **Regional Internet Registries (RIRs)** grew over time, and today there are five:

- African Network Information Centre (AfriNIC), covering Africa
- American Registry for Internet Numbers (ARIN), covering the United States, Canada, several parts of the Caribbean region, and Antarctica
- Asia-Pacific Network Information Centre (APNIC), covering Asia, Australia, New Zealand, and neighboring countries
- Latin America and Caribbean Network Information Centre (LACNIC), covering Latin America and parts of the Caribbean region
- Réseaux IP Européens Network Coordination Centre (RIPE NCC), covering Europe, Russia, the Middle East, and Central Asia

Each RIR has the authority within its region to administer and register IP address space and manage services related to IP addresses. The registries are not-for-profit, self-regulatory and self-funded organizations; like ICANN, they have open leadership structures to encourage direct participation by any Internet stakeholder.

Each of the RIRs has been engaged in encouraging and training its members to deploy the newest communications protocol, **Internet Protocol Version 6 (IPv6)**, for global cybersecurity purposes. IPv6 was developed by the IETF in anticipation that the Internet's supply of IP addresses would run short. IPv6 instantly solves the world's urgent shortage of computer addresses, and also supports better security features than IPv4, including mandatory support for **Internet Protocol Security (IPSec)**. IPSec is a tool used not only to encrypt Internet traffic, but also to authenticate it, which, in theory, could help law enforcement and counterintelligence agencies solve the ongoing problem of anonymous cyber attacks.

However, human rights groups fear that governments will use IPv6 to quash political dissent by reducing online anonymity and privacy. In short, next-generation Internet technologies such as IPv6 can redress some of the Internet's current security shortcomings, but the dynamic and rapidly evolving nature of the Internet and the threats against it, combined with external political factors, virtually guarantees that no solution will be a silver bullet for cybersecurity.

Cyber Fact

Because the Internet is a massively complicated international enterprise, it is important that the information traveling along it follow certain "rules of the road." On the Internet, the rules governing data communications are defined by organizations such as ICANN and IETF.

The Internet Engineering Task Force: Role and Responsibilities

The IETF is a loosely self-organized group of volunteers who contribute to the engineering of Internet technologies. It is the principal body engaged in the development of new Internet standards. The IETF is unusual in that it exists as a collection of activities, new technologies, and events, but is not a corporation and does not have a board of directors, members, or dues. The group hosts meetings and convenes working groups, including a Working Group on Web Security, to fulfill its stated mission: to "make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet."

Like other Internet organizations, the IETF encourages anyone from the Internet community to participate in its work. IETF is an "open standards" organization that has no formal membership or membership requirements. This openness and willingness to work through collaboration is truly astonishing, especially given that the Internet was originally created by the DOD, an organization with many confidential aspects to its work.

The IETF's stated mission is "to make the Internet work better by producing high quality, technical documents that influence the way people design, use, and manage the Internet." These documents are also referred to as **Requests for Comments (RFCs)**.[11] RFCs cover a broad range of content and can serve a variety of purposes—some RFCs propose new Internet standards, while others provide summaries of working group meetings. Sometimes, the IETF even has a bit of fun with its RFCs—for instance, RFC 2795, published on April 1, 2000, proposed the creation of an "Infinite Monkey Protocol Suite."

The name "Request for Comments" expresses an important principle behind the IETF's work: the Internet is a constantly changing technical system, and any document published today may need to be updated and improved tomorrow. It also reflects the IETF's philosophy that the best new knowledge is generated through open and collaborative efforts.

Indeed, one way to look at the IETF is as the group of people who work together to improve the technology of the Internet on a daily basis. In addition to producing RFCs, the IETF serves as a forum where network operators, hardware and software creators, and researchers can communicate with each other and ensure that future protocols, standards and products will be better than those that exist today. Therefore, IETF is the forum where the basic technical standards for Internet protocols, including IPv6, are set and maintained.

Issues and Challenges in Global Cybersecurity

The Problem of Attribution

The greatest single advantage a computer hacker has over international protocols, technical breakthroughs, and security standards is anonymity. Hackers hide within the maze-like architecture of the Internet and route attacks through a variety of well-chosen countries. For a hacker, "well-chosen countries" means countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation. This strategy typically allows more than enough time for a hacker to erase any evidence of an attack. According to security experts, the average time between an initial computer intrusion and its discovery is over 400 days.[12]

As a result, positive attribution and identification of an attacker is very difficult in cyberspace. This **"attribution problem"** has a number of implications for cyber attack victims:

- It reduces the possibility that a government or organization can deter, prosecute, or retaliate against a cyber attacker.

- It increases the odds that attacks will take place during peacetime with little or no warning.
- It encourages “false flagging” operations, where the attacker tries to pin the blame on an innocent third party.
- It creates an environment in which even terrorists can find a home on the Internet.
- It offers the attacker an additional layer of plausible deniability.
- It forces decision makers to respond to cyber incidents based on a preponderance of evidence, rather than clear and convincing evidence.
- It means that positive attribution can often only be determined from non-cyber data points, such as those drawn from traditional law enforcement, counterintelligence and espionage.

Lack of Transnational Authority

There are multiple organizations and sub-organizations across the globe devoted to confronting, tracking, and analyzing cyber crime. Despite this commitment of resources and manpower, the inability of the international community to designate jurisdictions, command authority, and communicate between organizations hinders the security of global cyberspace.

The jurisdiction of any nation-state’s law enforcement institutions ends every time a network cable crosses a border. Hackers routinely create enormous headaches for police and counterintelligence personnel by routing attacks through countries with which the victim has few established ties. The transnational nature of cyber crime, such as when a French hacker targets a Chinese company from a U.S.-registered computer, makes it difficult for any single organization to collect sufficient digital evidence against a cyber criminal.

Investigators must be able to articulate the activities of cyber criminals to criminal courts with authority and credibility. In order to do this, there must be clear legal guidelines that allow national agencies to work effectively with international partners. Currently, these guidelines do not exist. This presents a challenge significant enough that it is overcome only in rare cases or when there is an extraordinary international political interest in solving a case.

Amazingly, a common hurdle for international organizations is the simple problem of not knowing whom to call in the event of a cyber attack. This problem is compounded many times over when cultural, linguistic and nationalistic biases get in the way. And because many countries do not have data breach laws, organizations and businesses that suffer cyber attacks may not want to, and may never have to, disclose the attack to any authority figure.

Another challenge for international cybersecurity operations is that governments instinctively fear any perceived loss of national sovereignty. They may worry that cooperation in cybersecurity matters will allow foreign governments to obtain digital evidence through remote and unauthorized search and seizure, even though this would run directly counter to international law.

Yet another challenge mirrors the challenges we discussed in Chapter 2 (Cybersecurity Law and Policy). This challenge is the persistent tension between security and freedom in national security operations. Civilian organizations can have difficulty understanding the reasons for national security requirements. Governments, for their part, may be uncomfortable with the openness of the international Internet. A government that restricts network connectivity or abuses its law enforcement powers runs its own set of unpredictable risks, such as a low-probability but high-consequence scenario of a “hacktivist” group threatening the government’s network.

The United Nations and Cybersecurity

The U.N., with its 193 member states, represents the highest level of international cooperation and is the largest international organization in the world.

There are two principal U.N. efforts regarding cybersecurity: a politico-military stream focusing on cyber warfare and an economic stream focusing on cyber crime. The U.S., Germany, Canada, and U.K. have been active players in this dialogue, with a vocal Russia playing the role of primary counterweight to U.S. power. One concrete achievement of this dialogue has been the U.N.'s sponsorship of a conference series called the World Summit on the Information Society (WSIS), which has produced several outcome documents. On the U.N.'s official website, the researcher will find many official statements and speeches on international cyber crime and cybersecurity.

The North Atlantic Treaty Organization (NATO) and Cybersecurity

In terms of international peace and security negotiations, no organization can match the experience and legitimacy of NATO. Since its 1949 formation in the turbulent aftermath of World War II, the purpose of NATO has been the collective defense of its member states. NATO links Europe with North America and has a formal dialogue with dozens of additional nations. NATO's Article 4 provides for consultation and coordination in response to any external security threat. Article 5 states that "an armed attack against one … [is] an attack against all," and supports every member state's right to defend itself.

Before 2010, information technology played no role in NATO's Strategic Concept, and cyber attacks were not recognized as a national security concern. But the 2007 Estonia crisis transformed NATO's thinking. Suleyman Anil, head of cyber defense in NATO's Emerging Security Challenges Division, stated that "Estonia was the first time...[that we saw] possible involvement of state agencies; [and] that [a] cyber attack can bring down a complete national service, banking, media…"[13]

Therefore, in 2008 NATO began to write its first Cyber Defense Policy. In 2010, NATO's new Strategic Concept described cyber attacks as threatening "Euro-Atlantic prosperity, security and stability." Currently, two NATO priorities are to bring every element within the organization under centralized cyber protection and to accelerate the expansion of the NATO Computer Incident Response Capability (NCIRC), a partner organization of US-CERT. Today, NATO policy calls for a crisis-response team of cybersecurity experts to be sent to any member state that is a victimized by a damaging cyber attack.

The Council of Europe and Cybersecurity

The most important international cyber legal agreement to date is the Council of Europe's **Convention on Cybercrime**, issued in 2001 and now signed by 53 nations, including the U.S. This treaty is the only binding international agreement related to cybersecurity and is considered a template for any country wishing to develop comprehensive national legislation on cyber crime. Signatories meet each year for consultations, and the Council of Europe helps governments to ratify, accede, and implement the treaty through cooperative projects. The council's website is an excellent source of documents on cybercrime from an international law perspective.

Conclusion

The key to conducting effective cybersecurity research is to know the field's most influential research sources. Throughout the late 20th century and early 21st century, the U.S. government has been the world's leading producer of significant cybersecurity statements and legislation. The U.S. continues to cooperate with, coordinate, and partner with leading technological and security organizations to combat the growing threat of cyber crime. Cybersecurity as an academic field may have come to maturity in the United States, but it is quickly transforming itself into a field with an international orientation, as open as the Internet itself.

Key Questions

1. Article I of the U.S. Constitution established which branch of the federal government?

   a) The executive branch

   b) The legislature branch

   c) The judicial branch

2. In the United States, what is the role of a grand jury?

   a) Delivering a verdict of innocence or guilt

   b) Sentencing a convicted criminal

   c) Determining probable cause for a criminal trial

3. Which of the following is NOT part of the Executive Office of the President (EOP)?

   a) The Office of Management and Budget (OMB)

   b) The National Security Council (NSC)

   c) The Department of Defense (DoD)

4. What is the complex question fallacy?

   a) Posing a question that is too difficult to answer

   b) Posing a question based on a questionable assumption

   c) Posing a question that may have multiple answers

5. In the U.S., how do the Federal Sentencing Guidelines work?

    a) Judges assign point values to crimes, and determine the appropriate punishment based on a crime's point value.

    b) Judges determine punishment based on international standards set by the United Nations Security Council.

    c) Judges allow juries to suggest appropriate punishments for convicted criminals, and determine the final sentence according to the jury's unanimous suggestion.

6. Which President made public some aspects of the CNCI?

    a) President Obama

    b) President Bush

    c) President Clinton

7. What event directly preceded Presidential Decision Directive 63?

    a) The terrorist attacks in the U.S. on September 11, 2001

    b) The discovery of the Stuxnet attack on Iran's nuclear facilities in June 2010

    c) The Oklahoma City bombings of 1995

Cyber Connections

Many examples of cyber crime and punishment in this chapter bear significant links with the narratives presented in the Introduction to this book. The U.S. government's role as the world's leading institution on matters relating to the global Internet and its secure operations was also evident in the introductory narratives. Because the Internet was originally a project of the DOD, its security has always been a project of the U.S. government.

The laws and policies discussed in this chapter have roots in the historical events examined in Chapter 2. This chapter may be considered a companion to Chapter 2 and offers the structural backdrop to the events discussed in that chapter.

The technical aspects of the global Internet are a primary concern of organizations such as ICANN and the IETF. The technical concepts and Internet vulnerabilities discussed in Chapter 4 are major concerns of these organizations.

The laws governing the cybersecurity operations of private sector organizations in the United States may prove influential as international cybersecurity efforts increase in the coming years and decades. Understanding the concepts discussed in Chapter 5 will help any student of developing international cyber law and policy. Furthermore, the private sector's roles and responsibilities with regard to U.S. national security will only increase in the years to come, and it is likely that new U.S. cybersecurity laws and policies for the private sector will emerge in the near future.