THE GREAT COURSES®

Topic
Science & Mathematics

Subtopic
Computer Science

Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare

Course Guidebook

Professor Paul Rosenzweig
The George Washington University Law School

PUBLISHED BY:

THE GREAT COURSES
Corporate Headquarters
4840 Westfields Boulevard, Suite 500
Chantilly, Virginia 20151-2299
Phone: 1-800-832-2412
Fax: 703-378-3819
www.thegreatcourses.com

Paul Rosenzweig, J.D.
Professorial Lecturer in Law
The George Washington
University Law School

Professor Paul Rosenzweig is a Professorial Lecturer in Law at The George Washington University Law School, where he lectures on cybersecurity law and policy. He also serves as an Adjunct Professor in the Near East South Asia Center for Strategic Studies at the National Defense University. In 2011, he was awarded a Carnegie Fellowship at Northwestern University's Medill School of Journalism, where he returned as an Adjunct Lecturer in the fall of 2012.

In his nonacademic endeavors, Professor Rosenzweig is the founder of Red Branch Consulting, PLLC, a homeland security consulting company, and a senior advisor to The Chertoff Group. He formerly served as Deputy Assistant Secretary for Policy in the U.S. Department of Homeland Security, and he is currently a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute. Professor Rosenzweig is a Senior Editor of the *Journal of National Security Law & Policy* and a Visiting Fellow at The Heritage Foundation.

Professor Rosenzweig is a cum laude graduate of The University of Chicago Law School. He has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography (a department of the University of California, San Diego) and a B.A. from Haverford College. Following graduation from law school, he served as a law clerk to the Honorable R. Lanier Anderson III of the United States Court of Appeals for the Eleventh Circuit.

Professor Rosenzweig is the author of the recently released *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, coauthor of *Winning the Long War: Lessons from the Cold*

War for Defeating Terrorism and Preserving Freedom, and coeditor of *National Security Law in the News: A Guide for Journalists, Scholars, and Policymakers*. ■

Table of Contents

Table of Contents

Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare

Scope:

Since first developed as a research project in the 1960s, the Internet has grown to become a world-girding, borderless domain where more than 2.5 billion people buy goods, consult doctors, foment rebellion, send photographs, and do countless other things both big and small. With that powerful openness, however, comes grave insecurity. The goal of this course is to teach you about the structure of the Internet and the unique threats it breeds. In the end, this course will center on a single overarching theme: that Internet openness brings risks and dangers that cannot be eliminated, but they are risks that can be understood, managed, and reduced. By the end of the course, you'll have a greater appreciation for what governments and individuals can do and are doing to reduce those threats.

Our course begins with a case study—of the Stuxnet virus that attacked Iranian nuclear production facilities. Some think of Stuxnet as the world's first cyber guided missile. It is the first instance we know of where cyber attacks had real-world physical effects. However you characterize it, this new reality will be transformative. The interconnectedness between the cyber domain and the physical world creates new vulnerabilities and poses new legal and policy challenges. The disruption of settled assumptions and expectations is, in some ways, reminiscent of the sea change we saw in world governance after the introduction of nuclear weapons. Our goal will be to explore challenges posed by the dynamic changes in cyberspace in a systematic way.

The course continues by looking at fundamentals and basic structures. We will learn first how the Internet and cyberspace are built and why they are built the way they are. It turns out that a good deal of vulnerability is built into the system from the start. The Internet would not be the network we know if it were structured in a more closed and secure way, but that lack of security is a critical gap that can't be technologically fixed. We'll also spend some time looking more closely at the different types of viruses

and vulnerabilities that infect the cyber domain. You will gain a better understanding of the difference, say, between Trojan horses and botnets.

After that, we'll close the introductory portion of the course by trying to get a feel for who the different actors are in cyberspace. We'll learn that there is a world of difference between the motivations of, say, China or the United States and those of cyber hackers, and those are very different from the motivations of organized crime actors in cyberspace.

In the second part of the course, we'll look at some of the issues of law and policy that are bound up in our dealing with these threats. We'll begin by examining the prospect of government regulation of the Internet and asking whether or not it can be effective. Then, we'll investigate the even more problematic (and challenging) question of international cooperation. Because the Internet spans the globe, some international governance is essential, but what should it look like? We will also discuss how the Constitution both protects our civil liberties and possibly limits our ability to protect ourselves. We'll ask some questions about encryption policy as a way of protecting ourselves, and we'll take a dive into the topic known as "big data"—the idea that everyone leaves a trail in cyberspace. What we will discover is that almost every aspect of cybersecurity is a double-edged sword: New technologies can be used to foster freedom but also to create greater insecurity.

The third part of the course steps back from our look at particular policies to put the problem in context. Anticipating that some form of cyber attack will inevitably succeed, we'll take a look at how to make the entire network more resilient so that we can recover from an attack. We'll also look at how to make yourself a less inviting target and provide a short catalog of tips on how you can better protect yourself. Finally, we'll do some crystal-ball gazing, looking at what the next 10 or 20 years may hold for us in the cyber world.

Stuxnet—The First Cyber Guided Missile

Lecture 1

In July 2010, a computer security firm in Belarus announced that it had discovered the signature of a new piece of malware—malicious computer software. This announcement was not unusual or surprising. After all, the cybersecurity firm Symantec discovered more than 400 million new pieces of malware in 2011, most of which were easily identified and rendered harmless. But this new virus—Stuxnet—was different; it was the harbinger of a changed world. Up until this software was developed, many experts believed that the effects of cyber conflicts would be restricted to the cyber domain. As we'll see in this lecture, Stuxnet showed the world that cyber war could potentially kill real people.

A Two-Phase Attack

- Stuxnet caused a malfunction in the centrifuges used in a uranium purification facility in Natanz, Iran. What's frightening in that statement is that there is nothing that limits a cyber assault to this type of facility or process. The type of system invaded in Iran also controls the heat of nuclear reactors. It would be no harder to cause the centrifuges to break down than to pull out the graphite control rods, causing a nuclear meltdown.

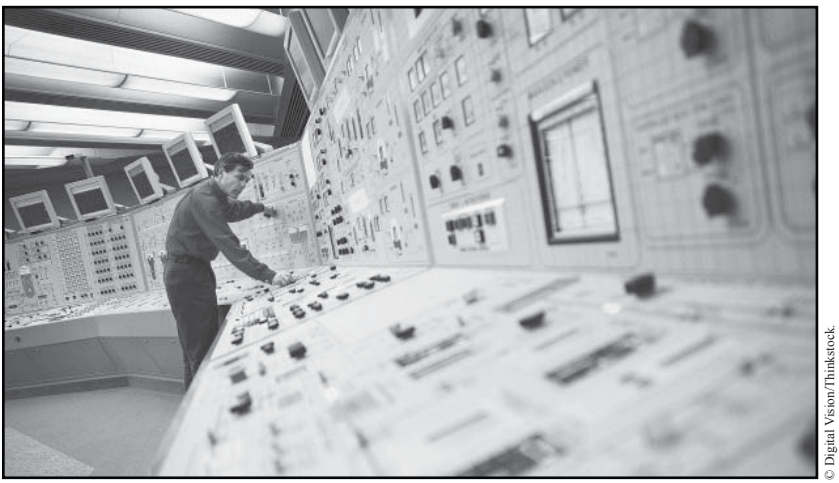
- Stuxnet used a two-phase attack. In the delivery phase of the program, the **malware** infected a Windows-based Microsoft operating system. The purpose of this delivery phase was to put the attack program in a system that might someday be attached to the target's control system.

- From this delivery platform, the malware was designed to "jump" to infect what is known as a **SCADA** system—a supervisory control and data acquisition system—manufactured by the German firm Siemens. This jump from the Microsoft operating system to the SCADA system was the attack phase of the program.

- The program required two phases for its attack because many SCADA systems that run sensitive or secret machinery are not directly connected to the Internet. A direct connection makes a system more vulnerable to intrusion; thus, operators add an additional layer of security by creating an "air gap," a measure designed to ensure that there are no connections between the system and the Internet.

- The Iranian nuclear enrichment program was almost certainly air gapped from the broader Internet. Stuxnet must have entered the SCADA system through some interaction with an external, Windows-based program. No one knows for sure how that happened.

- The second phase of the attack demonstrated a high degree of sophistication. It was designed to target only a particular type of operating program. In identifying its target within the Iranian nuclear enrichment facility, Stuxnet's developers exhibited a significant degree of inside knowledge.



Stuxnet may have been introduced into the Iranian control program when an engineer hooked up a Windows-based tablet for diagnostic purposes, or it might have been purposely introduced by an industrial spy.

- Stuxnet manipulated the speed of centrifuge rotors used in the process of purifying uranium, causing variations that were designed to slowly wear down and, ultimately, crack the rotors. Because the centrifuges ran at a variable rate, the uranium produced by the facility was impure and unsuitable for use. Stuxnet also disabled and bypassed several digitally operated safety systems designed to ensure that the centrifuges ran at a fixed speed.

- Ultimately, Stuxnet was a piece of computer malware that had a real-world effect. Any physical system that is operated by a computer system was now at least theoretically vulnerable to attack and possible destruction.

- Not only did Stuxnet have physical effects, but it also hid them! Buried within the program was a prerecorded series of false data reports, leading operators to believe that the centrifuges were running normally.

- Though Stuxnet was targeted at an Iranian facility, according to Symantec, by September 2010, there were 100,000 computer servers infected with the **virus** around the world, including in the United States.

- Responsibility for the Stuxnet malware has not been decisively demonstrated, although some people believe that hints buried in the malicious code point to Israeli authorship. *The New York Times* reported that Israel and the United States cooperated to produce Stuxnet, and according to the *Washington Post*, Stuxnet was the last phase of a U.S.-Israeli cyber sabotage program known as Flame.

A Decisive Change

- In July 1945, when the first experimental atomic bomb was exploded, J. Robert Oppenheimer, the scientist who led the Los Alamos development effort, immediately recognized the destructive power of the bomb and the transformative effect it would have on war-making. But neither Oppenheimer nor anyone else could,

at the dawn of the nuclear age, anticipate the long-term social, psychological, and geopolitical effects of this development.

- Of course, we now know that the first atomic bomb brought us nuclear power and cheaper electricity, but it also brought us new ways of thinking about war, such as the concept of mutually assured destruction.

- In the broader field of world geopolitics, nuclear weapons also wrought unexpected changes. The existence of atomic weapons mandated a policy of containment rather than confrontation because nuclear war was too grave to risk. From this policy flowed the Cold War, the Marshall Plan, NATO, and ultimately, limited wars in Korea and Vietnam.

- At the beginning of the nuclear era, all these developments were unanticipated by anyone who witnessed the first atomic explosion.

- The dawn of the cyber age is no different. We have had an easy time exploiting the benefits of the Internet, but now it seems as though vulnerabilities threaten to outweigh those benefits. The Internet is a wild and dangerous place, where our secrets and even our identities are increasingly at risk.

- Stuxnet was a proof of concept that cyber war can be real. And as the Department of Homeland Security recently noted, now that information about Stuxnet is publicly available, it's much easier for other bad actors to develop variants that target other SCADA systems around the world. Because SCADA systems are pervasive and generic, the Stuxnet **worm** is, essentially, a blueprint for a host of infrastructure attacks.

- The American demonstration that nuclear weapons were capable of manufacture assured the Soviets that their efforts would eventually succeed. Similarly, the proof, through Stuxnet, that cyber attacks can have kinetic effects has opened up a world of possibilities for malware designers, many of which are potentially catastrophic.

- It's also possible that the damage to Iran's nuclear program caused by Stuxnet was just a useful collateral benefit to a larger purpose: that of sending a message to the Iranians that even their most sensitive programs were vulnerable. This is sometimes called an "info hack," in which the purpose is more to let opponents know that they are vulnerable rather than to achieve any particular result.

- The most profound similarities between atomic weapons and cyber threats, however, lie in the disruptive nature of the Stuxnet event.
  - Imagine what it must have been like the day after the first atomic bomb was exploded. Around the globe, settled assumptions about war, policy, foreign affairs, and law had, in an instant, all come unglued. Even 17 years after the atomic bomb was first exploded, the uncertainty about the use of these weapons and the threat they posed was so great that the Cuban missile crisis nearly engulfed the world in nuclear war.

  - We are on the verge of experiencing that same sort of tumultuous time, and almost nobody in America—except a few senior policymakers—knows it.

  - Perhaps more ominously, even at the dawn of the nuclear age, we were confident that we could identify anyone who used atomic weapons, and they would all be peer nation-state actors. In the cyber realm, we have much greater difficulty identifying who "fires" the weapon, and the culprit may well be a non-state actor—perhaps terrorists or a small group of hackers.

- In short, we stand on the threshold of a new world, much as we did in 1945. From this vantage point, nobody can say where the future might lead. But we do know that the changes that lie ahead will affect everyone on the planet.

Overview of the Course

- The binary system of counting, which uses only 1s and 0s, lies at the heart of the cyberspace revolution. Every bit of data is expressed as a string of 1s and 0s. In physical terms, deep within the innards of

the computer, silicon chips create those 1s and 0s through a series of transistors whose structure is etched into wafer-thin silicon integrated circuits.

- The beauty and genius of cyberspace lie in recognizing the universal power of these simple 1s and 0s. The rapidity with which they can be manipulated has, over the past decades, increased exponentially. And that explosion in computing power has fostered an explosion of new technology. Hardly a day goes by without the development of some new computer application (an "app") that is intended to enhance our lives.

- America's increasing use of, and dependence on, technology for our social infrastructure is changing how we live our lives. The pace of our technological advances has significant implications for how individuals interact, how the economy functions, how the government and the private sector conduct business, and how we protect our national interests and provide for our common defense.

- Cyberspace is everywhere, and it's part of our everyday activities. But precisely because it is so pervasive, our dependence on cyberspace creates new risks and dangers. This course will explore how we can reap the benefits of productivity and information sharing that come from a globalized web of cyber connections while reducing the damage done by bad actors who seek to exploit that globalized web for their own reasons.
    - We will start by looking at how the Internet and cyberspace are built and why they are built the way they are. We'll also spend some time looking at the different types of viruses and vulnerabilities that are infecting the cyber domain, and we'll try to get a feel for the actors in cyberspace.

    - In the second part of the course, we will look at some of the issues of law and policy that are bound up in our handling of these threats. We'll ask some questions about encryption policy as a way of protecting ourselves, and we'll dive into the topic

known as “big data”—the idea that everyone leaves a trail in cyberspace for others to see and use.

- The last part of the course steps back a bit from particular policies and tries to put the problem in context. We’ll look at how to make the entire network more resilient and how you can protect yourself. Finally, we’ll try to peer into the future to see what the next 10 or 20 years may hold for us.

Important Terms

malware: Short for “malicious software.” A general term describing any software program intended to do harm.

SCADA (supervisory control and data acquisition): SCADA systems are used to control industrial processes, such as automobile manufacturing. They can be, but are not necessarily, controlled by other computer operating systems.

virus: A piece of computer code that infects a program, much as a virus infects a person, and replicates itself.

worm: A stand-alone program that replicates itself. It often hides by burrowing in and concealing itself amidst other program code, like a worm in dirt.

Suggested Reading

Alperovitch, *Revealed: Operation Shady RAT.*

Combating Robot Networks and Their Controllers.

Information Warfare Monitor, “Tracking GhostNet.”

Symantec, W32.Stuxnet Dossier.

Questions to Consider

1. How pervasive is the Internet in your life? How much do you think society has come to depend on the Internet?

2. Which do you think transformed human society more, the Industrial Revolution and steam power or the Information Revolution and the Internet?

The Incredible Scope of Cyberspace

Lecture 2

Every minute of every day, roughly 3 million Google searches are performed. In the same minute, 12 websites are hacked. The scope of the Internet is immense, and we can't truly understand cyber vulnerabilities, cybersecurity, and cyber warfare if we don't understand how cyberspace is built and why it works the way it does. In this lecture, we'll explore that topic and see how the scale of the Internet affects the scale of our vulnerability.

The Structure of Cyberspace

- Much of what we consider vulnerability in the Internet is inherent in its design. Indeed, the Internet is so effective precisely because it is designed to be an open system.
  - The networks that make up cyberspace were built for ease of communication and expansion, not for security. At its core, the logic layer of cyberspace is fundamentally dumb; it is designed to do nothing more than transfer information quickly and efficiently.
  - This fundamental simplicity is the key to understanding cyberspace.
- Although many users tend to think of cyber connections as nothing more than a glorified telephone network, the two are, in fact, structurally very different.
  - Telephone networks are hub-and-spoke systems with intelligent operation at central switching points. Phone calls come in from a user to a central switching system, where sophisticated switches route them from one caller to another, creating a single, end-to-end connection.
  - That structure means that the control of the system lies with the central authority—and that is also where the vulnerabilities

are. For example, in the world of telephone communications, intercepting a communication is as simple as going to the central switching station and attaching two alligator clips to the right wire.

- We should also note that you can't just join the telephone network; in effect, you need someone's permission. The centralized system controls your access and your services.

- Communications through cyberspace are completely different, though portions of them often travel over telephone lines. Put simply, there really isn't any central place to go on the network, and there is no central authority that runs it.

The Logic Layer

- When we talk colloquially about cyberspace, we're talking about the logical network layer where all the information gets exchanged. A map of all the connections involved here would look like a massive tangle of lines—a giant web built by a crazy spider.

- How do the 1s and 0s we talked about in the last lecture move around in this logic layer? Unlike the telephone system, where the information stays together in a single unit as it moves from one end of the conversation to the other, in the logic layer of cyberspace, the information to be transmitted is broken into small packets. These packets are separately transmitted along different routes and then reassembled when they arrive at their destination.
  - Thus, in contrast to the phone network, the cyberspace network is truly a "web" of interconnected servers that do nothing more than switch packets of information around the globe.

  - This web is, as we shall see, far broader than the "World Wide Web" of pages that you can navigate to. It is a much vaster web of interconnections of everything ranging from cars and power plants to webpages and cell phones.

- Transferring these packets of information requires very little intelligent design. All that is needed is an addressing system and a protocol for moving information from one address to another.
    - The addressing system is known as the **domain name system** (DNS) and the transmission protocol is known as the Internet protocol suite or, more commonly, the TCP/IP (transmission control protocol/Internet protocol).

    - We can think of the DNS as the Yellow Pages—a place to look up someone's address. The Internet protocols are rules about how to share information—how to identify the address in transit and how to package the information.

- As long as a user follows the TCP/IP, his or her information will be delivered—whether it's a recipe for apple pie or the code to launch a nuclear attack. The logic layer is nothing more than 1s and 0s being directed around a network.

- The real intelligent operations occur at the edges, on our mobile devices and laptops running various apps. You can, quite literally, hook on to the network any system that manipulates data in any way and outputs data as its product.

- What makes the Internet so successful is that access to it is not controlled at a central switching point. You don't need "permission" to add a new functionality. Anyone with a new idea can add it to the network by simply purchasing a domain name and renting server space. This simplicity and flexibility is what has driven the explosive growth of the Internet.

The Power of the Internet

- A simple example of a Google search demonstrates the power and transformative nature of cyberspace. Consider the search query: "Yankee second baseman 1973." What happens to find the answer to that query?

- First, the small text file of the query is translated by a web browser into a string of 1s and 0s for transmission across cyberspace. At the same time, another portion of the web browser picks out the correct **IP address** to which the question should be addressed.

- The question is then broken into several distinct packets of information for transmission, each of which takes a different track across the Internet before being reassembled at a Google server.

- At the Google server, the 1s and 0s are translated back into a natural language message. Then, sophisticated programs interpret that message, and data-processing algorithms identify which webpages are the most likely ones to have the answer.

- That list is immediately coded as a webpage, which is again reduced to 1s and 0s, broken into packets, sent across the Internet, and reassembled on the user's computer. All of this happens in under a second.

- Google didn't need permission to provide this service; the user was free to choose a service other than Google; and the user didn't have to buy the service from a central switching station. Access comes because Google chose to provide it, and any of us can use it by virtue of our connection to the network. The ability to choose services, to choose a method of access, and to ask questions of a universal nature across the entire scope and domain of the world is what makes cyberspace truly a worldwide web of connections.

- The distributed structure of the network also means that anything can be a node in the network, that is, an endpoint where the network connects to a function of some sort. In fact, anything with an IP address is somewhere on the cyberspace network: a cell phone, a car that has OnStar, smart-grid electric meters, and so on. The problem with this interconnection is that all of these nodes are potentially quite vulnerable.

A Five-Layer Cake of Connections

- The interconnections we've been discussing are part of the logic layer of the cyber domain, where the 1s and 0s are transmitted from server to server. But this logic layer is only one piece of the puzzle. Although most people think of cyberspace as limited to the Internet, its full structure is more complex. The logic layer is embedded in a much larger cyber domain, which we can conceptualize as a five-layer cake of connections.
    - At the bottom is the "geographic layer," that is, the physical location of elements of the network. Though cyberspace itself has no physical existence, every piece of equipment that creates it is physically located somewhere in the world. As a consequence, the physical pieces of the network are subject to the control of many different political and legal systems.

    - Next is the "physical network layer"—the hardware and infrastructure of cyberspace, all of which is connected. The components we think of in this layer include all the wires, fiber-

The damage caused by earthquakes highlights the real-world presence of cyberspace; in 2006, a quake cut undersea telecommunications cables and disrupted Internet traffic to Japan, Taiwan, South Korea, and China.

optic cables, routers, servers, and computers linked together across geographic spaces. To be sure, some of the links are through wireless connections, but all of those connections have physical endpoints.

- Above these two real-world layers is the logic layer that we've already described. This is the heart of the network, where the information resides and is transmitted and routed.

- Above the logic network layer is the "cyber persona layer," which includes such things as a user's e-mail address, computer IP address, or cell phone number. Most individuals have many different cyber personae.

- Finally, at the top, there is the "personal layer," which encompasses the actual people using the network. Just as an individual can have multiple cyber personae, a single cyber persona can have multiple users, and it is often difficult to link an artificial cyber persona to a particular individual. The true maliciousness of the network comes to the fore at this level, where people choose to act in malevolent ways.

- One of the greatest cognitive difficulties in coming to grips with vulnerabilities on the network is that policymakers, legislators, and citizens simply don't understand just how big the Internet is. The statistics are so sizable that they tend to overwhelm human conception.
  - As of late 2012, there were more than 2.5 billion Internet users. It is said that no other voluntary human endeavor has ever been this large.

  - Every day, those users conduct more than 3 million Google searches, engage in 11 million "instant message" conversations, and post nearly 700,000 Facebook status updates. According to Google's CEO, "Every two days, we now create as much information as we did from the dawn of civilization up until 2003."

- With the growth of information also comes a growing threat to our security. Every minute, more than 168 million e-mail messages are sent, and each one them is a potential threat and source of a malware intrusion. The scale of our vulnerability is exactly as great as the scale of the Internet.

- Perhaps even more significantly, the scale of the vulnerability comes with an immense governance problem. How can any human institution manage and regulate so large an enterprise? In many ways, that is the fundamental question posed in this course and the fundamental challenge of cybersecurity. In a system with this many participants, even if we had the right solutions for cybersecurity, how could we get the entire world to agree to carry them out?

Important Terms

domain name system (DNS): The DNS is the naming convention system that identifies the names of various servers and websites on the Internet. In any web address, it is the portion of the address after http://www. One example would be microsoft.com.

Internet protocol (IP) address: An IP address is the numeric address that identifies a website on the cyber network. Typically, it looks like this: 172.16.254.1. Using the IP address, information can be communicated from one server to another. One of the critical functions of the DNS is to translate domain names (which appear in English) into numerical IP addresses.

Suggested Reading

Gleick, *The Information: A History, A Theory, A Flood*.

Goldsmith and Wu, *Who Controls the Internet?*

Lessig, *Code Version 2.0*.

Zittrain, *The Future of the Internet and How to Stop It*.

Questions to Consider

1. If you wanted to destroy the Internet, how would you try to do it? Is it even possible?

2. When the Internet covers the entire globe, doesn't the question about how to manage and govern the Internet pretty much become a question of world government?

The Five Gateways of Internet Vulnerability

Lecture 3

As we discussed in the last lecture, the logical structure of cyberspace is a web-like one that is both a virtue and a vice. It's a virtue because it allows almost 100 percent accurate communications around the globe instantaneously. But it's a vice because the logic structure is about the communication of information and data—and only about communication. That focus on rapid, accurate, and effective communication—to the exclusion of other factors, such as security and identity—has made cyberspace a dangerous place. In this lecture, we'll take a closer look at this dangerous place and identify five distinct gateways that create vulnerability for anyone who connects to the cyber network.

Instantaneous Action at a Distance

- The history of human interaction is, essentially, one of increasing distance. Early in human history, such activities as armed conflict, sales of goods, malicious acts, and espionage required physical proximity. But over time, this necessity for proximity weakened. In warfare, for example, humans moved from using swords to bows and arrows, siege cannons and artillery, airplanes, and intercontinental ballistic missiles.

- The Internet is a quantum leap beyond that in capability. Now, action in the cyber domain occurs at the speed of light and crosses immense distances almost instantaneously. From your desktop, you can access a website in Japan, read a South American newspaper, or make reservations at a restaurant in Paris.

- But what is easy for you from your home computer is equally easy for any malicious actor in the world who wants access to a computer, say, in America. Whether the object is warfare, terrorism, espionage, or crime, it is no longer necessary for malevolent actors to be anywhere near the venue of their actions.

The Asymmetries of Cyberspace

- One of the unique features of the Internet is that the manipulation of bits and bytes does not require the development of a sophisticated industrial base, nor does it require a substantial financial investment. In other words, the barriers to entry into the cyber domain are incredibly low.

- Further, the structure of the Internet is such that, at least today, offense is much more effective than defense. As everyone knows, it's almost impossible to avoid a virus infection on your computer. **Firewalls** and intrusion detection systems are only so effective.

- That means that a small group of actors in cyberspace can have an incredibly large effect. A handful of intelligent hackers can compete in cyberspace against the most powerful nations in the world. The group known as Anonymous, for example, has taken down the CIA website and stolen internal e-mails from sophisticated security companies.

- Another example of this asymmetry can be found in the e-mail almost everyone has received from a Nigerian scammer, offering millions of dollars as a windfall if the recipient would only front a small transaction fee. Given that almost everyone recognizes such scams as frauds, why do they continue?

- The answer lies in the asymmetric nature of the Internet. Sending out 1 million scam letters is almost costless. Even if only one person in a million responds to the scam request, the disparity between the costs involved and the potential benefits to be gained from a successful scam make it highly profitable for the scammers to continue.

- This asymmetry in cyberspace is a radical development. In the past, fraud required significant opportunity costs—an investment of time, money, and energy by the con man. When a large investment is required, the actors want a relatively high degree of confidence that they will be successful. But on the Internet, fraudulent actors

can spend literally pennies with a realistic hope of reaping a financial reward.

- Another way of looking at the problem of asymmetry is through the prism of national security.
  - In the physical world, a country's power is judged by its force of arms. Few other countries can even come close to wielding the same nuclear power as the United States, for example. But the asymmetry of information power on the Internet changes that dynamic.

  - Such countries as North Korea and Iran are perfectly capable of challenging and perhaps even dominating America in cyberspace. The limits lie not in a nation's industrial base or the size of its economy but solely in the intellectual capabilities of its citizens.

Anonymity in Cyberspace

- Another disturbing fact about cyberspace is that we are sometimes not sure of the identities of our opponents.
  - The Internet was not designed to require identification. As initially conceived, its only function was to transmit information across great distances rapidly. That made sense at a time when there were only four nodes on the Internet, and everybody who used it knew one another.

  - Today, there are more than 2 billion nodes on the net, representing nearly a third of the world's population. It's incredibly easy to hide in that large a network.

- At the same time, the idea of anonymity on the Internet has become part of our culture. Many users, particularly in the younger generation, feel as though the freedom of the Internet is inherent to its development. In reality, that freedom is part of the architecture of the Internet and could be changed. Yet anonymity on the Internet has become a strong cultural norm, and it would be politically problematic to change the architecture of the system.

- The phenomenon of anonymity has also given rise to deliberately anonymous actors on the Internet. In addition to hackers operating collectively, criminal networks take advantage of the power of anonymity, operating almost with impunity around the globe.
  - One reason identity thieves are almost impossible to deter is that their own identities are almost impossible to discover.
  - Here again, the contrast with the physical world is remarkable. The requirement of physical proximity to commit a crime means that there are many opportunities to discover the perpetrator's identity—fingerprints, license-plate numbers, and so on. This is not true on the Internet.

- The lack of identification—what's called the problem of attribution—is one of the foundational difficulties of the network. Not only does it create the difficulty of defending yourself from unknown attackers, but it also raises a barrier to effective cooperative action with people or entities that you might actually want to work with, such as your bank.

- Identification isn't absolutely impossible to achieve, but it can be extremely difficult. In one case of cyber spying known as GhostNet, it took more than a year of exceedingly difficult forensic work to identify the source of intrusion.

- Anonymity has an inherently contradictory nature. The Internet offers a potentially dangerous kind of anonymity, but as we'll see in a future lecture, the footprints that the ordinary user leaves are indelible, and errors in judgment about what one views

If an anonymous individual or group were to disrupt the New York Stock Exchange from cyberspace, it might take a year or more to identify the perpetrators.

or posts can follow one forever. Bad actors are much harder to identify and track than innocent users.

Lack of Borders

- There are no border checkpoints on the Internet. The many packets of data in even a simple e-mail message cross multiple borders, but there is no easy way to control that flow of information.

- This is a deeply disorienting phenomenon. We're used to a world in which a sovereign nation can control its own border traffic, but that's almost impossible on the Internet. This lack of control is threatening to the entire structure of the international community.

- Since the Peace of Westphalia in 1648, sovereign nations have been defined by their ability to control territory and the transit of people and goods across that territory. Now, ideas and information flow across boundaries almost without limit, disrupting settled expectations and threatening the status quo.

- As a result, sovereign countries are desperately trying to re-create borders in the Internet domain, and any success they may have is only the result of limits in the architecture of the network.
    - China has developed a fairly strong set of controls over Internet traffic to and from the mainland. But those controls rely on the fact that there are only three major undersea cable arrival points for Internet traffic to the Chinese mainland.

    - Likewise, island nations, such as Australia and New Zealand, have limited connectivity to the broader network and are more readily able to control traffic to and from their citizens than, say, France or Germany.

    - In contrast, the United States has almost innumerable connections with the global network. In effect, every computer in America is a border-crossing checkpoint, but one that's outside the control of the government.

The Difficulty of Distinction

- The uniformity of 1s and 0s in the logic layer of the Internet is what makes the magic of cyberspace information transmission possible, but all the 1s and 0s look the same. Different types of activities in the logic layer are difficult to distinguish. We can't tell what any given piece of computer code will do just by looking at it.

- The code that does harm in a piece of malware is called the payload. This is the executable portion of the program that tells an intrusion what to do.
  - Once inside a computer, a program can steal, change, or destroy data; order the computer to send out spam; or, as we saw with Stuxnet, cause physical damage to a system it controls. But it's virtually impossible to tell in advance whether a particular piece of code is an innocent e-mail communication or a full-scale cyber attack.

  - Particular pieces of malware have unique signatures that allow us to distinguish them from innocent Internet traffic, but we usually come to recognize them only after the first attack has occurred. Thus, the initial attack will almost always get through. The only alternative is to treat all Internet traffic as malicious, and that's too difficult and intrusive to carry out.

Nightmare Scenario

- Here is the nightmare that plagues America's planners: Someday, we will discover malicious code in the systems of the West Coast electric grid. We won't know who put the code there, and we won't be sure of what the code is supposed to do.

- The attack will be at a distance, asymmetric, and anonymous. It will ignore borders, and it will lack distinction. Those are the five fundamentals of vulnerability on the network.

- What's most frightening of all is that these vulnerabilities are basic to the Internet system we've built; they are part of the reason that

the Internet has been so successful. That means there is no way to completely eliminate the problem.

Important Terms

firewalls: Computer security systems designed to prevent intrusions.

Suggested Reading

Baker, *Skating on Stilts*.

Bowden, *Worm: The First Digital World War.*

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

Rosenzweig, *Cyber Warfare*.

Questions to Consider

1. Which of these five gateways to vulnerability is the most unsettling to you? Why?

2. If we started over again in building the Internet, what characteristics that are missing would you want built in?

Of Viruses, Botnets, and Logic Bombs

Lecture 4

The first known virus to infect a personal computer was named Brain.A. It was developed by two Pakistani brothers and was initially detected in January 1986. The virus changed a file name on the computers it infected, causing them to freeze in some cases. How the world has changed since then! In just one generation, we have gone from novelty to very real threats in cyberspace. In this lecture, we'll learn about the instruments that are used to exploit the five Internet vulnerabilities we discussed in Lecture 3—botnets, Trojans, and logic bombs—and try to estimate the scope of the problem of cyber crime.

Distributed Denial-of-Service (DDoS) Attack

- A **distributed denial-of-service (DDoS)** attack is a common frontal assault on the Internet. Such attacks are relatively easy to mount but less harmful than some other types of assaults.

- The DDoS attack takes advantage of the fact that even though the cyber network is huge, it is still limited physically. Any one company has only so much bandwidth and so many servers. In a DDoS attack, a malicious actor floods a website with requests to connect, drowning out legitimate requests and, in effect, shutting down the site. Only access is affected in this type of attack; nothing happens to the data at the target company.

- A DDoS attack is carried out by a distributed network of helpers. If you volunteer to join the attack, you download a free program known as the Low-Orbit Ion Cannon (LOIC). With this simple automated program, you enter the web address or server you want to attack, hook up to the Internet, and push start to flood the target with requests to connect. If enough people join the attack, the target can be completely cut off.

Botnets

- We tend to think of attackers as having volunteered to join a DDoS attack, but in fact, not everyone is a volunteer. With **botnets**, many DDoS attacks are carried out by computers that have innocent owners. The term "botnet" is short for "robot network," essentially a network of controlled computers.

- Botnets work by infecting innocent computers with some piece of malware that then connects to a controller computer for instructions. If there are no instructions, the malware does nothing until its next scheduled check-in time. But sometimes, the command-and-control program sends out a message: "At precisely noon GMT on July 4, try to connect to GlobalMegaCorp.com." At the appointed time, all the computers connected to the broader web will follow the instructions.

- This is also how scammers arrange for spam to be sent; they rent out botnets from the herder (the owner of the botnet) and buy e-mail addresses that have been "harvested" on the web by an automated program called a "spider" or "web crawler."

- Botnets can vary in size, from hundreds to tens of thousands of computers. Most of them are constantly active, sending spam or engaging in some other malevolent activity literally every second of every day.

- Besides sending spam, botnet malware programs usually also try to spawn themselves by infecting other innocent computers, typically through an e-mail message or some other innocent form of communication.

Trojans

- A Trojan or **Trojan horse** is a computer program or message that, on the outside, looks like an innocent piece of code but contains a malicious piece of software.

- Usually, an attack begins with the simple communication, often an e-mail. This is called a **spear-phishing** e-mail, because it targets a specific individual or recipient, much like a spear used to catch a fish. These spear-phishing e-mails are designed to appear as though they have come from an innocent source, but they have a malicious program hidden in either the e-mail itself or an attachment.

- When the recipient clicks on the attachment, the malware begins the automated download of a controller program. This program then opens up a back-door communication channel, allowing outside individuals to access the programs that control the target's system.

- Some of the attackers create new breaches in the system; others use their position to give themselves authority to access all of the available data. If it is a hit-and-run attack, the attacker may remove information from the target system, such as log-in codes or financial data.

- Another class of attacks, called advanced persistent threats (APTs), are intrusions that reside inside the target system for a long period of time and make the target computer vulnerable to continuous monitoring from the outside.
  - An APT called GhostNet was found in March 2009 in the computers operated by the offices of the Dalai Lama.

  - Acting remotely, the installers of this malware could turn on a **keylogger**—a program that captures all the keystrokes entered on a keyboard attached to a computer. They could, for example, capture the organization's bank account passwords.

  - Also remotely, those who controlled the malicious software were able to turn on the video cameras and microphones on the computers in the offices of the Dalai Lama. They could see and hear anything that was happening within range of the computer.

  - It took an information warfare organization in Canada more than a year to unravel the chain of controlling computers and

find out who was behind the GhostNet attack. In the end, the chain petered out in servers on Hainan Island off the coast of China, the home of one of the signals intelligence organizations of the People's Liberation Army.

Logic Bombs

- Sometimes, the object of an intrusion isn't monitoring for information at all. Sometimes, the attack is intended only to leave a package behind, a program that sits quietly in the computer doing nothing at all, waiting.

- When it finally get the signal to act—perhaps from outside, or perhaps the program has a preset day and time—it will explode into action. Such silent programs are called **logic bombs**.

- One of the major concerns of security experts today is that we don't really know whether there are any logic bombs in some of our networks—and there's no way to find out.

Zero-Day Vulnerability

- A **zero-day exploit** is one that the attacker is sure will work because it has never been used before. The vulnerability becomes known on the same day that the attacker uses it to take advantage of someone. In other words, there are zero days between when the vulnerability is discovered and when it is used.

- In cyberspace, most vulnerabilities are gaps in programming code that, when discovered, can be exploited by outsiders. It's not surprising that such gaps or mistakes exist in programs that have millions of lines of code, such as the operating system for Windows. But certain flaws allow outsiders to force the code to take unanticipated actions, often with adverse consequences.

- Once a vulnerability is exposed and exploited, it can be fixed by software designers. That's why software security firms are constantly shipping updates to your computer, and software developers are constantly recommending that users download

patches for their software. They are providing you with the "fixes" to vulnerabilities that have recently been discovered, most often because some malicious actor has taken advantage of them.

- But new vulnerabilities—ones that have not yet been exploited—are a valuable commodity for bad actors. They can be used for important attacks because they are unlikely to have been patched and will almost surely work. Using at least one of these zero-day exploits is standard in more sophisticated attacks; Stuxnet used four—a sign of the importance the developer placed on the success of that attack.

In June 2012, a group of researchers hijacked a drone by fooling the GPS onboard the aircraft—a reminder that everything that is attached to the network and addressable is vulnerable.

Defending against Attacks

- It's important to note that the good guys can and do use the same tools as the bad guys. In order for the Canadians to track the GhostNet attack to China, they put malicious tracking software into some of the computers that were intermediaries for the attack. These programs allowed the Canadians to put "beacons" on the network traffic as a means of tracing it.

- Another particularly useful tool of the defenders is the "honeypot"—a computer that poses as an innocent but isn't. Such computers allow defenders to capture new malware before it infects others. In a similar vein, "spam traps" are systems designed to collect and analyze spam so that your filters know how to stop it.

The Extent of Cyber Attacks

- How significant is the problem of cyber attacks today? Although this question is a vital one, data on actual vulnerabilities and their effects are hard to come by. We don't even have good information about the number of intrusions that happen on a daily basis; it's such a large number that the U.S. government stopped counting several years ago.

- One massive study of Internet traffic conducted for Bell Canada in 2010 demonstrates the scope of the problem. In this study, investigators observed about 80,000 zero-day exploits per day in Canada alone and estimated that more than 1.5 million compromised computers attempted more than 21 million botnet connections each month. These data are more or less consistent with estimates by large cybersecurity companies elsewhere.

- But knowing that there is a lot of activity isn't the same as knowing what the effects there are. As a 2011 paper produced by PayPal noted, "Estimates of the magnitude and scope of cyber crime vary widely, making it difficult for policymakers and others to determine the level of effort to exert in combating the problem." And what is true of cyber crime is true, to an even greater degree, of instances of cyber espionage.

- The data we have on cyber crime tend to be unsatisfactory. In 2011, the U.S.-based **Internet Crime Complaint Center (IC3)** received more than 314,000 complaints of Internet crime, with reported losses of $485 million. These modest numbers pale in comparison to more apocalyptic estimates of malfeasant activity on the Internet. The last estimate of the U.S. Government Accountability Office (made in 2005) was that the annual loss due to computer crime was approximately $67.2 billion for U.S. organizations.

- One other way of trying to estimate the scope of the cyber crime problem would be to examine how much is spent in preventing intrusions and theft. After all, businesses wouldn't spend more in prevention than they anticipate in losses. The Internet Security

Alliance has estimated that private-sector security spending totaled an astonishing $80 billion in 2011.

- In the end, we don't know for sure what the scope—the actual dollar damage—of cyber crime really is. The most that can be said is that a lot of risk is out there, and that data about actual harm remain painfully elusive.

Important Terms

botnet: A network of computers controlled by an outside actor who can give those computers orders to act in a coordinated manner, much like orders to a group of robots.

denial-of-service attack: An attack in which a malicious actor repeatedly sends thousands of connection requests to a website every second. The many malicious requests drown out the legitimate connection requests and prevent users from accessing the site.

distributed denial of service (DDoS): A DDoS attack is related to a denial-of-service attack, but in a DDoS attack, the attacker uses more than one computer (often hundreds of distributed slave computers in a botnet) to conduct the attack.

Internet Criminal Complaint Center (IC3): The IC3 is a unit of the U.S. Department of Justice. It serves as a central collection point for complaints of criminal cyber activity and provides estimates of criminal effects.

keylogger: As the name implies, a keylogger program is one that records all the keystrokes entered on a keyboard (such as the letters and numbers in a password) and then reports those keystrokes to whoever installed the program.

logic bomb: A program that tells a computer to execute a certain set of instructions at a particular signal (a date or a command from outside, for example). Like many bombs or mines, the logic bomb can remain unexploded and buried for quite some time.

phishing: Phishing is a cyber tactic that involves dangling "bait" in front of an unsuspecting user of the Internet. The bait may be an e-mail with an attractive link to click on that takes the unwary user to a malicious site.

spear-phishing: A phishing attack that is targeted at a particular, specific recipient; the name comes from the similarity of using a spear to catch a particular fish.

Trojan horse: As the name implies, a computer program or message that, on the outside, looks like an innocent piece of code. Contained within the code, however, is a malicious piece of software.

zero-day exploit: A vulnerability in a software program that has not previously been used or discovered. Because most vulnerabilities are quickly patched after they become known, zero-day exploits, which are not yet patched, are valuable to malicious actors. They leave systems open to intrusions that will be successful on the "zeroth" day.

Suggested Reading

Baer, Heron, Morton, and Ratliff, *Safe.*

Baker, *Skating on Stilts*.

Chesney, "Military-Intelligence Convergence and the Law of the Title 10/ Title 50 Debate."

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

George and Rishikof, eds., *The National Security Enterprise.*

Rosenzweig, *Cyber Warfare*.

Schmitt and Shanker, *Counterstrike*.

Questions to Consider

1. Which is more dangerous to you personally, a targeted spear-phishing attack or a DDoS attack on your bank? Which types of attack are more threatening to national security?

2. Given the uncertainties in the data, do you think people are making too much of the threat? Are those who talk about a cyber–Pearl Harbor crying wolf?

The Problem of Identity on the Network

Lecture 5

Type the query "WHOIS" into a search engine, and you will see at least a half dozen links offering services that will, in theory, help you identify the people behind various domain names on the Internet. This seems like a wonderful service, almost like the Yellow Pages for Internet domain names. But it turns out that verifying a person's identity on the network is actually very difficult. In this lecture, we'll try to understand why that is so and what we might do to fix the problem, if it's even a problem at all.

Obscurity in Domain Names and IP Addresses

- In any web address, the domain name is the portion of the address after http://www. Domain names are familiar ways to identify the webpage you are trying to reach or the e-mail address to which you are sending a message.

- Of course, computers use numbers instead of names to route traffic. The domain name system (DNS) is, in effect, a translation system; it translates a domain name to an IP address, a numerical label assigned to every device on the network. The DNS/IP combination is both an identification system and an address system.

- The DNS link works in a three-stage process. First, an individual registers a domain name, which is hosted on a server somewhere. Second, the server is identified by an IP address. Third, when a user wants to access a website by typing in its domain name, the DNS programming routes the request to the right server and returns the webpage to the user.

- The addressing function of the DNS is critical. If the DNS were corrupted or hijacked, then communications across the Internet would break down. Maintaining a registry of which domain names are in use is also critical. This function is performed by the **Internet Corporation for Assigned Names and Numbers**

(ICANN), a nonprofit organization that sets the rules for creating and distributing domain names.

- In theory, the DNS should be completely transparent. Knowing a domain name (the "cyber persona" of a person or company), you should be able to find out who the real person behind the domain name is. Unfortunately, the system doesn't work as effectively as it should.

- The obscurity of the DNS makes it fairly easy to hide your identity. For example, for a relatively small amount of money, you can create a shell company registered almost anywhere in the world. You could then buy a domain name from a registry company, such as Go Daddy (which works with ICANN to organize the sale of domain names), and hide behind the shell corporation to conceal your identity.

- Because domain name registry companies accept identification that appears to be lawful and because they make no real attempt to verify the information they receive, the WHOIS registry is littered with errors, both accidental and deliberate.

Other Techniques for Masking Identity

- As we discussed in an earlier lecture, messages that transit the net don't automatically come with authentication. You may receive a message that purports to be from your friend, but it could be a spoof, that is, a communication intended to fool you. Almost everyone who uses the Internet has received at least one communication that's a fraud.

- Even worse, many techniques exist to confound efforts to backtrack a message to an original source. It is a relatively easy technical matter to gimmick an IP address so that a message appears to come from one location while actually coming from another.

- Further, in a world where botnets allow malicious actors to control computers other than their own, it is quite possible to originate a message from a computer that doesn't belong to the originating party.

- As a result, virtually every intrusion or attack on the network is obscured behind a farrago of false e-mail addresses, spoofed IPs, and botnets under the control of a third party.

Addressing the Problem of Attribution

- The difficulty of identification is perhaps the single most profound challenge for cybersecurity today, but it's not an insurmountable problem. As we saw with the GhostNet intrusion, the Information Warfare Monitor project was able to break into some of the hackers' own computers to follow the trail and, in the end, traced the origin of the intrusion to servers on Hainan Island.

- Such efforts demonstrate that attribution is a question of resources and permissions. If you are willing to devote enough time, money, and personnel to the issue and if you have permission to perform certain acts that, in other contexts, might be illegal, then attribution can ultimately be achieved. The major problem here is that such efforts tend to take a long time.

- The good news is that we are getting better at identifying malicious actors. In October 2012, Secretary of Defense Leon Panetta said that the DoD was beginning to see returns on its investment in addressing the problem of attribution. For example, the National Security Agency has identified roughly 20 separate Chinese networks of hackers that are causing most of the espionage damage in America today.

- It's important to note that many of the actors in cyber crime live beyond the reach of American law. They often can't be extradited and prosecuted. Likewise, though attribution gives us a better sense of when and how cyber espionage occurs, that knowledge doesn't make a diplomatic response any easier.

Trusted Identities

- If we accept that we can't achieve attribution by working backwards from the intrusion to the hacker, we need to invert the problem and try to establish identity at the human-computer interface.
  - What this means in practice is finding a way to make access to the Internet available through "trusted identities." Sometimes, this idea is caricatured as requiring a driver's license to use the Internet.
  - The idea here is to somehow control identity on the network when you sign on in a way that locks in an identity for tracking.

- In the United States, this trusted identity system would have to be voluntary. It is almost impossible to imagine that any system requiring mandatory identification would be politically acceptable, and such a system would probably be unconstitutional.

- Even a voluntary system, though, would be of some use. If you wanted to be careful, you could refuse to do business with any entity that didn't have a trusted identity. You could even create your own private networks with only trusted users.

- The trend toward trusted identification on the network can go a long way toward solving the attribution problem but at real cost to Internet freedom. We need to consider whether broader

Internet identification is a principal means by which China controls its citizens; the Chinese government also regulates access to Internet cafes.

American interests are advanced by the widespread adoption of trusted identity rules. Trusted identity can enhance security, but in authoritarian countries, Internet identification could be a way of suppressing dissent.

- Some network engineers are working to keep the Internet free with such tools as Tor, a free software program designed by The Tor Project. Tor is an anonymizing tool used by journalists, human rights activists, hackers, law enforcement officers, and others. It encrypts messages and uses a volunteer network of servers around the globe to "bounce" encrypted traffic in a way that evades detection. Tor protects privacy for individuals and secrecy for governments, but it can also be used by criminals to conceal their actions and identities.

Domain Name System Security Extension (DNSSEC)

- One major effort in trying to make identity on the network more easily verifiable is the **domain name system security extension (DNSSEC)**. Under DNSSEC, a new authentication security feature would allow users to be sure that when they attempt to connect to a domain name, such as whitehouse.gov, they are reaching the true whitehouse.gov website and not a facsimile. Basically, each website (or e-mail address or other device) would come with an authentication certificate.

- One benefit of this type of system is that it would eliminate "man-in-the-middle" attacks. Those are attacks where the malicious actor steps into the middle of a conversation and hijacks it by making independent connections with the victims. From the middle vantage point, the third party can relay messages between the victims, making them believe that they are talking directly to each other over a private connection, when in fact, the entire conversation is under outside control.
    - For example, without DNSSEC, your request to connect to your bank could be redirected to a phony website. There, the malicious actor could record your bank password before passing it on to the real bank. Because you actually make the connection to your real bank, you never know there's a

problem, and the thief can return to the bank website after you log off and access your account.

- Once DNSSEC is deployed, however, a "security resolver" function will be built into web browsers to check the authentication certificates of websites.

- DNSSEC sounds like an easy answer, but it is difficult to accomplish for a number of reasons.
  - First, DNSSEC must be backward compatible; in other words, it has to work even with portions of the Internet that have not deployed the new security protocols. Otherwise, changing over to DNSSEC would disconnect you from the broader web.

  - Second, there is a substantial cost for upgrading and deploying DNSSEC across a global range of servers and systems. The process will take years to complete.

  - The biggest difficulty is establishing a "chain of trust" for domain name authentication. At some point in the chain of authentication, there must be an original root authentication that serves as a "trust anchor." Currently, the trust anchor is provided by ICANN, but some people outside the United States don't trust this American company.

- Of course, if there is a chain of trust to establish identity for domain names, we can also be sure that bad actors will seek to undermine it. That happened in July 2011 when a hacker claiming to be an Iranian student penetrated a certifying authority in Holland and generated false certificates for real companies and government agencies. In the end, the only way to beat this attack was for the web browser manufacturers to revoke all the certificates issued by the certifying authority.

- The promise of robust attribution and identification is a bit of a chimera. Attribution is clearly possible in many cases, but it is also clear that creating a world of trusted and secure identities on the

network is a nearly impossible dream. We can make a great deal of progress in some aspects of the effort, but in the long run, we need to understand that anonymity is a feature of our current Internet architecture, not a bug.

Important Terms

domain name system security extension (DNSSEC): A proposed suite of security add-on functionalities that would become part of the accepted Internet protocol. New security features will allow a user to confirm the origin authentication of DNS data, authenticate the denial or existence of a domain name, and ensure the data integrity of the DNS.

Internet Corporation for Assigning Names and Numbers (ICANN): A nonprofit organization that sets the rules for creating and distributing domain names. Originally chartered by the U.S. government, it now operates on a multilateral basis from its headquarters in California.

Suggested Reading

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

Executive Office of the President, *National Strategy for Trusted Identities in Cyberspace.*

Rosenzweig, Paul, *Cyber Warfare*.

Questions to Consider

1. If the United States had a voluntary trusted identity system, would you join?

2. Most Americans are happy to trust ICANN to run the naming network. Most of the developing world isn't. Why do you think that's the case?

Cyber Fraud, Theft, and Organized Crime

Lecture 6

We can think of conflict in cyberspace as structured something like a pyramid, with frequently occurring but moderately harmful activities at the base and rare threats that would have catastrophic consequences at the top. In this lecture, we'll look at the base of this pyramid, which includes cyber scams and fraud that involve the theft of money or identity. These activities may not be as catastrophic as a cyber war, but for individuals who are injured, the consequences are all too painful and real. In the end, we'll see that cyber crime is quite similar to crime in the real world: endemic and pervasive, but we'll also look at how law enforcement authorities are fighting back.

Cyber Fraud

- What's known as the 419 scam is nothing more than the computer version of an old-time fraud called an "advance fee scheme." Here, the victim is offered an "opportunity" to share in a windfall if only he or she will provide the scammer with a small advance to pay for fees. Many of us are familiar with the cyber version of this crime through an e-mail requesting help in illegally transferring money out of Nigeria.

- Three factors make the cyber version of this scam especially effective: First, the anonymity of the Internet makes the scammer practically invulnerable to identification. Second, extradition is unlikely because Nigeria doesn't sympathize with American victims. Finally, the near-costless nature of the Internet allows the scammer to send out thousands of fake solicitation e-mails, counting on the fact that at least a few people will respond.

- The Nigerian scams seem so blatantly false that we tend to think that only someone who is truly naïve would respond, and that's exactly the point. The scammers are trolling for the naïve so that they don't have to waste time cultivating their marks.

Identity Theft

- Like the 419 scam, the problem of identity theft isn't conceptually new either—a waiter could always steal your credit card number—but if you use your credit card in cyberspace, there are many new ways in which your identifying information can be stolen.

- We saw the man-in-the-middle attack in the last lecture. Another endemic problem today is that your personal information, including your credit card number, is often held by others—banks, supermarkets, and online stores. That means that your identity is only as safe as the least safe company you work with. Data theft from such businesses is now so common that we actually have a new set of laws to deal with data breach.

- To limit your likelihood of being a victim, make sure you use a secure encrypted connection whenever you send personal information to a company on the web; look for the closed-lock symbol in most browsers. You should also give out less information on the web; don't store your credit card number with online retailers.

Organized Crime

- One example of organized crime on the web is the Russian Business Network (RBN). The RBN was an Internet service provider run by criminals for criminals. It is said to have been created in 2004 by a programmer who is the nephew of a well-connected Russian politician.

- The RBN provided domain names, dedicated servers, and software for criminals on the Internet. It was sometimes called a "bulletproof network" because, in effect, users were capable of hiding their criminal activities and were invulnerable to prosecution or discovery in their countries of origin.

- To a large degree, the RBN was just another business. It offered access to protected servers for $600 per month and highly effective malware, priced at $380 per 1,000 targets. All this came with

free technical support, patches, updates, and fixes. Typically, such bulletproof hosts have many customers, such as phony pharmaceutical manufacturers and child pornography websites. They can also often act as centralized control servers for various botnets, some of which they rent out at bargain-basement prices.

© Keith Brofsky/Photodisc/Thinkstock.

"Operation Blitzkrieg," the attempt of a cartel of Russian organized crime hackers to simultaneously attack 30 American banks, has been discovered, but similar operations may remain undetected.

- In its heyday, the RBN was responsible for some of the largest criminal hacks to date. One example is the infamous Rock Phish scam, in which users were tricked into entering personal banking information on the web, resulting in losses of more than $150 million. The RBN is also said to have provided some support for Russia during its conflicts with Estonia in 2007 and Georgia in 2008.

- Under severe pressure from the Russian government, the RBN officially closed its doors in 2008, though many suspect that its offices simply moved to another location.

Economic Espionage

- Yet another type of cyber crime that still resembles traditional crime in some way is economic espionage, that is, spying directed at economic secrets rather than secrets related to national security.

- According to the U.S. Office of the **National Counterintelligence Executive** (NCIX), the threat of economic theft is pervasive. In an

October 2011 report, NCIX detailed some of its conclusions: "U.S. private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, [and] Russia's intelligence services are conducting a range of activities to collect economic information and technology from U.S. targets."

- This activity is both a cyber crime and, at the extremes, a significant threat to national security. At some point, economic espionage (especially of companies in the defense industrial base) blends into national security espionage, and criminality becomes spying.

Illegal System Intrusions

- One problem we confront in cyberspace is the problem of building new definitions, and that is particularly true when we try to define the crime of an illegal intrusion into a computer system without the authorization of the computer owner. It seems obvious that it ought to be a crime to hack into someone else's computer, but the problem is in defining what that means.

- In the United States, the controlling law in this regard is the Computer Fraud and Abuse Act (CFAA), which makes it a crime to access a computer without, or in excess of, authorization. Again, this seems logical, but how do we determine the limits of "authorization"?
    - Because this term is not defined in the law, the courts have looked to contractual agreements that govern the use of a computer or Internet system. These agreements are known as the terms of service (ToS)—what you "accept" before you sign up for, say, a Facebook account. This means that private corporations are, in effect, establishing what conduct violates federal criminal law.

    - Here's what that means in practice: Three U.S. federal courts have said that an employee can be prosecuted under the CFAA if he or she exceeds an employer's acceptable use policies for the company network. An employee who works for an

employer who limits "personal use" of the Internet can, in theory, be prosecuted for accessing, say, a fantasy football league webpage.

- This new rule creates "computer crimes" for activities that are not crimes in the physical world. If an employee photocopies an employer's confidential document to give to a friend without the employer's permission, there is no federal crime (though there probably is a contractual violation). However, if an employee e-mails that document, that's a CFAA crime.

- It may be that we are comfortable with relying on prosecutorial discretion to decide when and when not to prosecute everyday wrongs as crimes, but it seems at least a little strange that the law can be used to prosecute someone for, say, telling a fib on a dating website (which is against the rules for most sites).

- Another problem with the CFAA is that under this law, it's probably illegal for a company under attack to defend itself effectively. In fact, many of the most reasonable actions that a private-sector actor would take in defense of its internal network are likely to violate the CFAA.
  - Under the CFAA, it is a crime to intentionally access a computer without authorization, but the most successful defensive measures often involve using "beacons" or other forms of surveillance inside the bad actor's computer to identify the source of the attack, in other words, putting code into an attacker's computer to trace the attack. Once an attacker is identified, another effective countermeasure might be to "flat line" his or her IP address, that is, arrange for it to be taken down.

  - These types of defensive countermeasures, sometimes going by the name "hack back," are probably crimes under U.S. law. Almost invariably, any protective action by a private-sector actor will involve accessing a computer without the authorization of its owner (who may sometimes even be an innocent intermediary) and obtaining information from it.

Thus, almost every aspect of private-sector self-help is, in theory, a violation of the CFAA.

Law Enforcement Measures

- One measure law enforcement can use to cut off a criminal network is what is known as an *in rem* ("against the thing") action. Such legal actions can be taken against a thing, such as the servers controlling a botnet, rather than a person or a company. The virtue of an *in rem* action is that you do not need to know who owns or controls the "thing"; you only need to know where the thing itself is.
  - In April 2011, in order to shut down a botnet, the U.S. government sought and received authority from the courts to send software commands to computers owned by private individuals in the United States that had been unknowingly infected.
  - This action was taken for a good cause and with court supervision, but it may be a bit frightening to think that the government could interfere with your computer usage.
  - The government has also used *in rem* proceedings to fight online piracy, that is, the illegal downloading of movies or music.
- More controversial are recent legislative efforts to combat piracy by requiring Internet service providers to divert traffic away from domain names that are identified as trafficking in stolen content.
- Unfortunately, these *in rem* tactics work only in the United States, while a large fraction of the criminal problem lies overseas. The reality is that cyber crime is predominantly transnational in character, which makes it difficult to solve and even more difficult to prevent. This situation turns our deterrence model of law enforcement on its head.
- To date, there has been only one real effort to develop an international approach to cyber crime: the Convention on Cybercrime, developed by the Council of Europe. The goal is to

ensure that there are no safe harbors for cyber criminals. But the process is slow; only 37 countries have ratified a treaty agreeing to cooperate in the transborder investigation of cyber incidents, and China and Russia are not among them.

Important Term

National Counterintelligence Executive (NCIX): Part of the Office of the Director of National Intelligence. The mission of the NCIX is the defensive flip side of our own espionage efforts. It is charged with attempting to prevent successful espionage against the United States by our adversaries.

Suggested Reading

Brenner, *America the Vulnerable.*

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

Rosenzweig, *Cyber Warfare*.

U.S.-China Economic and Security Review Commission, *Report to Congress.*

VeriSign, *The Russian Business Network.*

Questions to Consider

1. How much personal information do you share with places you do business with on the web? Can you reduce what you share?

2. Do you know anyone (such as your children) who regularly downloads movies or music? Why does downloading seem acceptable, but taking the DVD or CD from the store is something that nobody would ever do?

3. What diplomatic steps should the United States consider to convince other countries to be more helpful in combating cyber crime?

Hacktivists and Insurgency

Lecture 7

The word "hacktivism" is a combination of "hack" and "activism," and it suggests the use of computer hacking methods to stage a protest or make a political statement. In this lecture, we will enter the netherworld of hacker activists and cyber insurgency. In this shadowy realm, it sometimes seems as if there are as many different actors with different motivations as there are grains of sand on the beach. Because of this, it can be difficult to distinguish the good guys from the bad guys and, indeed, to determine when a noble motive becomes a criminal act. We will learn to identify some of the actors in this online realm, including political activists, cyber insurgents, and criminal mischief makers.

Cyber Insurgency

- Cyber insurgency is a little like war and a little like crime, with some political free speech thrown in for good measure. The fight most resembles what the military calls a "low-intensity conflict."

- Cyber insurgents may seem as if they are fighting a war in cyberspace, but often their "weapons" are simple cyber tools and the results of their actions are limited to the defacement of a website or denial of access.

- Cyber intrusions by non-state actors are not between sovereign nations; the actors don't have any territory to protect; and the hackers are practically immune from military retaliation. But because cyber insurgents are so hard to pin down, they pose a significant danger to stability. If their motives are sufficiently pernicious, we might think of them as cyber terrorists, but if their motives are purer, they might be considered cyber civil rights protesters.

WikiLeaks

- **WikiLeaks** is an organization dedicated to the publication of secret documents and confidential information. In 2010, it released more

than 250,000 classified State Department cables, along with other materials related to military actions in Afghanistan and Iraq.

- With its disclosure of classified information, WikiLeaks challenged state authority, yet one of the most significant responses to its activities came from the private sector.

- The combination of official government displeasure and clear public disdain for WikiLeaks' founder, Julian Assange, led a number of major Western corporations, including MasterCard, PayPal, and Amazon, to stop selling their services to WikiLeaks.

- What followed might be described as the first cyber battle between non-state actors.
  - Supporters of WikiLeaks—specifically, the loosely organized group of hackers called **Anonymous**—began a series of DDoS attacks on the websites of the major corporations that they thought had taken an anti-WikiLeaks stand. Anonymous also hacked the website of the Swedish prosecuting authority that was seeking Assange's extradition to face criminal charges.

  - The corporate sites used defensive cyber protocols to oppose Anonymous, successfully deflecting most attacks. An unknown group launched DDoS counterattacks on the website of Anonymous.

  - In short, a conflict readily recognizable as a battle between competing forces took place in cyberspace—and it was waged, almost exclusively, between non-state actors.

Anonymous

- This first cyber conflict ended in something of a draw, but Anonymous learned from this battle, and many of the group's subsequent attacks have shown more sophistication and effectiveness. The group has also made it clear that it intends to continue to prosecute a cyber war against the United States and other targets.

- Anonymous has posted a manifesto declaring cyberspace independence from world governments and called on U.S. citizens to rise up in revolt. In many ways, it conducts itself in the same manner that an armed insurgency might, even intercepting the communications of its enemies—international law enforcement agencies.

Loose groups of hackers, such as Anonymous, have demonstrated that they can do significant damage to individuals and companies, even with limited tools.

- One problem with the metaphor of war or insurgency, however, is that Anonymous and other groups like it are not monolithic. They have as many different agendas as they do people.
  - In some cases, these groups seem like **hacktivists** who have a political agenda, yet at other times, they seem like vigilantes or criminals. And sometimes, they seem as if they are just engaging in criminal mischief.

  - At still other points, hacktivists seem close to traditional political activists, fostering freedom of speech. For example, hacktivists provided technical assistance to the Arab Spring protestors and helped them evade authoritarian reprisals.

  - It's quite a challenge to get a handle on a group like this, when the actions of its members veer wildly from the extreme of participating in a near cyber war to supporting free speech for political dissidents.

Other Hacker Groups

- In the time since the initial Anonymous/WikiWar conflict burst onto the scene, a number of other organizations have surfaced that are

intent on disrupting Internet traffic as a means of expressing some political or sociological viewpoint. One of the most notorious of these was a splinter group known as LulzSec.

- This group claimed responsibility for a number of significant intrusions in 2011, including the compromise of user accounts at Sony, which affected millions of PlayStation3 users, and for taking a CIA website offline. By many accounts, LulzSec had no more than six core members, and some of their public posts suggested that they were motivated by a childish enthusiasm for creating disorder rather than by a more anarchic worldview akin to that of Anonymous.

- In June 2012, LulzSec announced that it was stopping its operations, perhaps in response to threats from other hackers to expose its members or perhaps as a result of the arrests of four suspected members in the United Kingdom and America.

- In 2011, a group called Inj3ct0r Team claimed that it had compromised a server belonging to NATO, removing confidential data from a backup server and leaving behind a scatological message in a Notepad file. As with some other groups, it is suspected that Inj3ct0r began as an individual effort and became a team as that individual attracted a group of loyal followers.

- There are also "good guy" hackers who fight the bad guys. Among these groups is a German organization known as the Happy Ninjas. In late 2011, the Happy Ninjas shut down a group known as carders.cc, which was a marketplace for stolen credit cards, drugs, and child pornography.

Crime or Protest?

- A thorny issue tied to the cyber intrusions of Anonymous, LulzSec, and similar groups is the challenge of drawing a line between impermissible crime and lawful activist protest. Many in the hacktivist community see themselves as part of a latter-day civil rights movement and view their denial-of-service attacks as similar to the sit-ins of prior decades.

- One lawyer representing a defendant who allegedly participated in an Anonymous denial-of-service attack on PayPal contends that even if the allegations are true, his client did nothing more than engage in a political protest that caused a minor inconvenience. And Eugene H. Spafford, a computer security professor at Purdue, likened the WikiWar to "a spontaneous street protest."

- For many people in America, this analogy resonates. Many people see the Internet as a global commons for political protest and watch with approval as Internet communication tools, such as Facebook and Twitter, are used to foster debate and dissent. There is reluctance to apply law enforcement principles to some of the insurgents' less disruptive acts.

- In the end, however, cyber insurgents also live in the real world; they cannot occupy only the cyber persona layer without also occupying the true persona layer. And therein lies the easiest means of responding to their tactics.
    - For some, such as the LulzSec members, the response may be arrest and criminal prosecution. Twenty-five members of Anonymous were likewise arrested in early 2012 by Interpol.

    - For other institutions, such as WikiLeaks, the physical-world response has also had a significant effect. By the second half of 2011, the financial pressures brought to bear on WikiLeaks by the cutoff of its traditional funding streams had led it to suspend operations entirely. Subsequent efforts to revive the brand have been fitful at best.

Service Providers as Insurgents

- On January 18, 2012, a worldwide protest by Internet service providers directed against a proposed set of online piracy laws shut down many portions of the web and modified many others. Sites participating in the protest included Wikipedia, Reddit, Google, craigslist, Mozilla, Imgur, and the Consumer Electronics Association.

- For our purposes, what these sites were protesting is less important than the mechanism they chose for conveying their message.
  - These are not the acts of insurgents in any classical sense of the term; these organizations weren't seeking to overthrow governments or start a revolution. But in many ways, both their ideology (for an Internet free of regulation and government interference) and their tactics (blocking or modifying Internet content access) are more than vaguely reminiscent of those adopted by some of the more radical Internet activists.

  - It seems that some of the most dynamic members of America's innovative corporate community can, when pressed, take advantage of their position at the center of all communications to advance their own interests.

  - This demonstrates that, in a real way, many levers of control in the cyber domain are now held by private-sector actors. Consider a scenario in which the owners of Verizon, Google, and Facebook were opposed to a war proposed by an American administration. They could pull the plug on Internet communications as an expression of their own views about world peace.

Authoritarian Nations and Non-State Actors

- We should not assume that every nation reacting to a cyber insurgency will do so in the same way. As practiced by Western nations, the fight against activists and insurgents has certain rules, but that's not necessarily the case around the globe. Some nations, such as Syria and Iran, can be quite brutal in their response to activism, including cyber activism.

- Adding even more complexity, non-state actors can also have varying degrees of respect for the rule of law and the conventions of conflict. When two non-state actors go after each other, almost anything is possible, as evidenced by the conflict between Anonymous and a Mexican drug cartel known as the Zetas.

- As with other insurgencies, the advantages held by cyber insurgents depend to some extent on Western nations' adherence to the rule of law, and those advantages may evaporate if an opponent declines to play by those rules. Though Western nations would never threaten brutal tactics, we can take steps to create real-world consequences for non-state actors who would otherwise face none.

Important Terms

Anonymous: A loose collective group of cyber hackers who espouse Internet freedom and often attack websites that they consider symbols of authority.

hacktivist: A combination of the words "hacker" and "activist." The term denotes a hacker who purports to have a political or philosophical agenda and is not motivated by criminality.

WikiLeaks: A website founded by Julian Assange. It accepts anonymous leaks of classified, secret, and confidential information and then posts the information in an effort to promote transparency. Controversial in operation, WikiLeaks' most famous leak was of more than 250,000 classified State Department cables.

Suggested Reading

Brenner, *America the Vulnerable.*

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

Rosenzweig, *Cyber Warfare*.

U.S.-China Economic and Security Review Commission, *Report to Congress.*

VeriSign, *The Russian Business Network.*

Questions to Consider

1. In your mind, what is the difference between the motivations of Anonymous and, say, the Russian hackers who attacked Estonia? Does that difference make a difference?

2. What is the best way to deal with the problem of hacktivists? Ignore them, treat them like criminals, or treat them like guerrilla fighters?

Nations at Cyber War

Lecture 8

We've yet to see an all-out cyber war in the real world and perhaps we never will, but as recent examples in the news indicate, nations are increasingly considering cyberspace as a separate domain for conflict. If we do have a cyber war, it is likely that the conflict will emerge as a collateral part of a true kinetic war. When and if a full-on cyber war begins, its destructive capacity may rival that of a physical conflict. In this lecture, we will try to define a cyber act of war and think about how we will know when (or if) we've been attacked. We'll also consider whether, when, and how a country can respond to a cyber attack.

Defining a Cyber "Act of War"

- We might consider certain acts of our adversaries, such as probing a Pentagon computer to map its structure and identify its vulnerabilities, as clearly analogous to espionage in the physical world. Thus, such an intrusion wouldn't be considered an act of war. In contrast, introducing a logic bomb to disrupt a military command-and-control system seems no different than a physical act of war.

- What about the middle ground? What if an adversary implanted a worm that slowly degrades GPS location data, reducing the accuracy of weapons that rely on those data? Is that espionage, or is it more like planting a bomb in another country's harbor in preparation for war?

- We have only begun to answer these questions. For now, the Pentagon has decided that the traditional "laws of armed conflict" apply in cyberspace just as they do in the physical world. Though this decision is not surprising, it is by no means clear that it will work out or even what it means in practice.

- For example, is the "battlefield" of cyberspace limited to geographic areas of military conflict, or does the U.S. Cyber Command have authority to execute military operations against adversaries wherever they may be? If al-Qaeda websites are hosted on servers in, say, Malaysia, are those servers military targets?

- More fundamentally, adopting the traditional laws of armed conflict defines an act of war as any act that is equivalent in kinetic effect to a military attack. Under this definition, an attack on the electric grid would be an armed attack if the cyber assault had the same effect as a missile attack might have.

- The logical consequence of this analysis, also part of the Pentagon's policy, is to authorize the U.S. military to use any weapon in its arsenal in response.

Russian Attack on Georgia

- The world has not yet seen a true cyber war, but the Russian attack on Georgia in 2008 is a close approximation.
  - In August 2008, Russian troops fought Georgian troops regarding a disputed border area between the two countries. During the course of that conflict, a number of cyber attacks were made on Georgian Internet services.

  - A DDoS attack prevented the Georgian Ministry of Foreign Affairs and other official Georgian sites from using the Internet to convey information about the attack to interested third parties. In other instances, cyber intruders corrupted the code for various official Georgian websites, defacing them with pro-Russian messages.

- According to the U.S. Cyber Consequences Unit, a nonprofit research institution, these attacks were carried out by Russian civilians (so-called patriotic hackers) who had advance notice of Russia's military intentions and the timing of its operations. The civilians were, in turn, aided by elements of Russian organized

crime. Additional evidence suggests that Russian intelligence agents may have coordinated the attacks.

- The attacks were effective, not only in preventing Georgia from getting its own message out to the world but also in disabling the Georgian government's ability to communicate with its people in order to respond to the Russian military invasion. These cyber attacks represent the first use of cyber weapons in a combined operation with military forces.

- Even in this context, however, it is not clear whether the attacks, standing alone, met the traditional definition of armed conflict. Though highly disruptive, it is difficult to say that their effect was equivalent to that of a kinetic attack. In the end, no physical damage was done; the actions are thought of as cyber war only because they were tied to the Russian invasion.

- The Russian-Georgian war demonstrates the limits of our practical knowledge about cyber conflict between nation-states. As we've said, in the cyber domain, the attacker may not be readily identifiable. In the end, the critical question in a cyber war may well be: Who attacked us? Although we have suspicions about Russian intent in the Georgian war, the reality is that we don't have conclusive identification of Russian responsibility.

- We also need to remember that what is good for the goose is, inevitably, good for the gander. Some have argued that Iran might view the Stuxnet virus as an armed attack, allowing it to use military means in self-defense. Later cyber attacks on a major Saudi oil corporation and several American banks have been viewed as Iranian responses to Stuxnet.

How Will We Fight in Cyberspace?

- Recall our earlier discussion about the lack of distinction in cyberspace. That problem, combined with the borderless nature of the Internet, can lead to a host of almost insoluble issues regarding the use of cyber force. A few of these issues are outlined below.

- International law allows the targeting of combatants who are participants in war. Killing armed combatants is a lawful act and is not murder. But who is a cyber combatant? Is a civilian hacker an armed combatant? How about a civilian employee with cyber responsibilities in a non-military government agency, such as the CIA? And what about the unwitting individual whose computer has been hijacked? If these individuals are combatants, then, in effect, the domain of lawful warfare is as broad and wide as cyberspace itself.

- Certain targets, such as hospitals, are immune from attack under international law. But IP addresses don't identify such facilities, and most server systems are inextricably intertwined with one another. How can a military attack ensure that it avoids damage to privileged targets? And if it cannot, does that mean that any cyber attack is illegal?

- Under the laws of war, combatants must carry their arms openly and be readily identified by uniforms. But most cyber warriors are not distinguishable from non-combatant civilians. Indeed, one of the principal tactics of a cyber warrior is to hide his or her actions behind the veneer of seemingly innocent civilian activity. Given that they don't abide by the laws of war, does that mean that cyber soldiers (like terrorists) are not entitled to the protections of those laws when identified or captured?

- The laws of armed conflict respect the rights of neutrals. In the cyber domain, however, successful attacks will almost always violate neutrality by using servers and computers that are located in a non-combatant country. Only a fool would, for example, make a direct attack from a U.S. server to one in China, yet due respect for the principle of neutrality suggests that this is precisely what is required by international law.

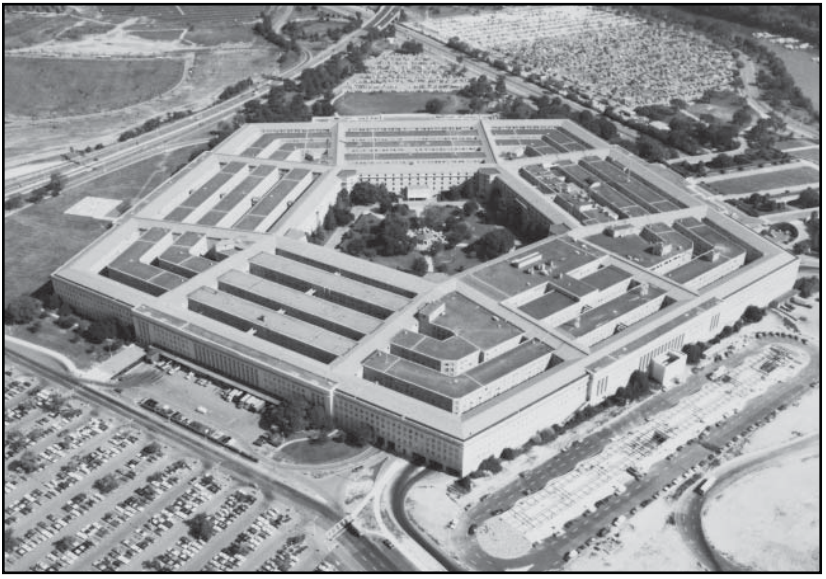
Centralization of Command and Control

- The nature of cyber operations—conducted at a distance—allows for the increasing centralization of command and control. In

other words, key targeting decisions are being made by more senior officials.

- It is difficult to overstate the significance of this change. In a physical war, decisions are typically made by a commander on the scene in relatively close geographic proximity to events. And legal judgments about proposed courses of action are made by military attorneys who are attached to combat units at the front and have situational awareness of the conflict.

- By contrast, when decisions about whether or not to launch a cyber weapon are made by a central authority and higher-ranking officials, we see an increasingly important role for lawyers. Many observers see this as a good thing, but it is likely to produce some odd results, such as the Justice Department's conclusion that U.S. cyber attacks cannot transit through servers in neutral countries.



Cyber weapons are often deployed with forethought and are part of a preplanned series of military actions; as such, they are far more likely to be controlled by senior authorities than is typical for a military engagement.

- Although there are benefits to centralizing command and control, the proximity to unwieldy bureaucracy also poses challenges for the management of military operations.

Who Are Our Cyber Enemies?

- The most effective national actor in cyberspace is China. As the Department of Defense's 2010 report to Congress concluded: "Numerous computer systems around the world, including those owned by the U.S. government, continued to be the target of intrusions that appear to have originated within the [People's Republic of China]. These intrusions focused on exfiltrating information, some of which could be of strategic or military utility."

- Among China's cyber incursions over the past few years are GhostNet, which we discussed in an earlier lecture, as well as Titan Rain and Byzantine Hades, the formerly classified code names given by the U.S. government to a series of coordinated attacks on American government and industrial computer systems.

- A different, more technologically troubling display of Chinese capabilities occurred in April 2010, when roughly 15 percent of the world's Internet traffic was routed—essentially hijacked—to China. In 2012, evidence suggests that someone in China attempted to "hack the patches" sent out by Microsoft to correct known software vulnerabilities.

- Perhaps most chillingly, in 2011, the security firm RSA was penetrated by an intrusion that compromised the company's SecurID system, which was, at the time, the single most common piece of security hardware in use by banks and private companies. A later attack on Lockheed Martin using the stolen RSA data seems a clear indication that the hack was done by a sovereign nation, and other evidence pointed to China.

- The Chinese government routinely denies awareness or responsibility for these activities, but no one who seriously studies the issue doubts that the attacks on American systems are part of

a campaign that could not occur without Chinese state approval. Further, what is true for China is also true of other nations and non-state organizations that have demonstrated equally threatening capabilities. In short, there is no lack of potential enemies on the horizon.

Suggested Reading

Brenner, *America the Vulnerable.*

Carr, *Inside Cyber Warfare.*

Clarke and Knake, *Cyber War.*

Libicki, *Cyberdeterrence and Cyberwar.*

Nye, *Cyber Power.*

Rosenzweig, *Cyber Warfare*.

Questions to Consider

1. Should U.S. policy support applying the traditional laws of war to cyber conflict, or should we pursue the development of a new set of rules? What do you think are the realistic prospects for agreement on new rules?

2. Do you think the enhanced role of lawyers in managing cyber war is a good thing or not? Why?

3. Should we treat China's pervasive espionage as an act of war?

4. What would be a proportional kinetic response to, say, an electric grid brown-out in Houston, Texas?

Government Regulation of Cyberspace

Lecture 9

We have just spent several lectures outlining all the vulnerabilities in the cyber domain and identifying all the bad actors—from criminals to other nations—who might want to cause harm in cyberspace. The question we must now address is: Can the cyber realm be made safer, and if so, how? As we will see in the next few lectures, society is slowly bringing order to the chaos of the cyber domain. But that may not be an altogether good thing; with order often comes control. In the next few lectures, we will explore various efforts to make cyberspace a safer place, starting with a look at the debate in America over government regulation of cybersecurity.

Why Regulate Cyberspace?

- Why do we need any security regulation of cyberspace? After all, we don't have regulations that require us to put bars on our windows or locks on our doors. Why do we need rules that require us to put firewalls on our computers? The most substantial reason we might need regulation is that our national security requires it.

- The U.S. Cyber Command and the National Security Agency are both located at Fort Meade in Maryland, and their primary source of electric power is a private company. A cyber attack on this company could result in significant national security concerns.

- Of course, the problem is not limited to Fort Meade and the Cyber Command. Across the board, our military response is critically dependent on cyber capabilities—for transportation, communication, and power. Thus, some see the lack of private-sector cyber protection as a problem that threatens our very existence as a nation.

- If the threat of what U.S. Secretary of Defense Leon Panetta called a "cyber Pearl Harbor" is real, why would we not want to take any

step—including regulation—to prevent it? Economic disruption on a grand scale would disable the U.S. government from responding to external threats.

- Note that this line of thought equates vulnerability with risk. Yes, vulnerabilities exist—even for critical infrastructure attacks—and the consequences of such an attack would be severe. But vulnerability isn't risk; there must be someone who actually wants to implement a threat and has the capability to do so. And right now, there aren't a lot of "someones" out there.
  - Stuxnet, for example, was not the product of a small-scale hacker group or terrorist cell. The extensive cyber espionage program required to map and exploit the vulnerabilities of the Iranian cyber systems was obviously the work of a nation-state. Do we really think that China would do something similar to the United States, especially given than we could then counterattack?

  - Certainly, vulnerabilities in critical infrastructure exist, but warnings about a potential cyber Pearl Harbor have been publicized since 1996. Right now, the only actors capable of a large-scale, crippling cyber assault are nation-states, and the likelihood that they will launch such an assault is roughly the same as the chances of a large-scale kinetic war.

  - As of now, the chaotic actors whom we might fear more, such as Anonymous or terrorists, don't have the capabilities to launch a crippling cyber assault. They will probably attain such capabilities in the future, but we don't know when that will be.

  - Without a better case for critical infrastructure catastrophe as a realistic possibility—not just a theoretical vulnerability—some are not persuaded that a cyber regulatory system is needed.

Economic Argument for Regulation

- Consider everything that you personally do in cyberspace, such as communicating through e-mails, getting directions on your iPhone, buying books from Amazon, and so on.
  - Now imagine giving all that up. How much money would it take to convince you to give up cyberspace completely?
  - The answer to this question, on average, is about $2 million, which we can translate to an annualized value of $40,000 for a 40-year-old individual. That's what economists would say is that individual's utility valuation of Internet access.
- Now consider how much you spend annually to get that access. You might spend $50 a month for a DSL line ($600 a year) and perhaps another $1,000 a year for a cell phone. In other words, you spend $1,600 a year for something you value at $40,000. That's quite a value proposition for cyberspace!
- Finally, how much do you spend protecting that investment? Maybe you have a firewall system that costs you $40 a year. That means, in some way, you think that your chances of being subject to an intrusion are less than 1 in 1,000 each year. By now in this series of lectures, you've probably figured out that you're kidding yourself.
- What if we change the perspective from you, personally, to all the public and private corporations and entities in our lives?
  - Consider what organizations do in cyberspace from a business perspective: keep records of government activity, communicate with constituents, track projects, store personal data on taxpayers or customers, operate infrastructure facilities, and so on.
  - If organizations were forced to do without the Internet, operational costs would skyrocket, yet businesses also systematically underinvest in Internet security, largely because, in the short term, it saves them money. This is what economists call an externality: when private goods cause public harms.

- Many cybersecurity activities have positive external effects. By securing your own server or laptop against intrusion, for example, you benefit others on the network, because your computer cannot be hijacked into a botnet and used to attack others. Indeed, almost every security measure performed in any part of cyberspace improves the overall level of cybersecurity by raising the costs of attack.

- But cybersecurity also has negative external effects, one of which is diversion. Most methods of protection, such as firewalls, have the effect of diverting attacks from one target to another. Any improvement in one actor's security is equivalent to a decrease in security for systems that are not as well protected.

© iStockphoto/Thinkstock.

Increased cybersecurity has a negative diversion effect: Any improvement in security for one user is a reduction in security for another user who is not as well protected.

- The second negative effect is a pricing problem that reflects a failure of the private market.
  - Sometimes, the price of a product doesn't have all the costs of the product built in. A typical example is air pollution, where the long-term costs from adding carbon to the atmosphere aren't part of the cost of the car or of the gasoline used to drive it. When such costs aren't included in the price of a product, the product is too cheap and somebody else winds up paying the costs in the end.

  - The costs of cybersecurity failures are similar. When software fails to prevent an intrusion or a service provider fails to stop a malware attack, Microsoft and Verizon don't bear the expense

of fixing the problem. Instead, the end user who owns the computer pays the costs.

- In general, no mechanism currently exists by which the software manufacturer or Internet service provider can be made responsible for the costs of those failures. In this way, security for the broader system of the entire Internet is a classic market externality whose true costs are not adequately recognized in the prices charged and costs experienced by individual actors.

- This is why some people think regulation is necessary: If the market isn't functioning, then it needs to be fixed.

How Would Regulation Work?

- The first step in establishing a new regulatory system would be to determine what it covers.
  - The basic idea here is that it would cover only cyber infrastructure connected to physical systems in which damage could have a major impact, such as a catastrophic interruption of life-sustaining services or catastrophic economic damage.

  - Deciding which systems are the most critical within a particular sector presents one problem. We can't say, for example, exactly which electrical systems are the most important.

  - Further, the act of creating a list of protected systems also creates a list of unprotected systems. As one expert has noted, this is "a bit like writing a targeting list [for] our opponents."

- Once we know what to protect, how do we decide how to protect it? One way might be for the federal government to set protection standards directly, but the government is too slow in writing rules and not nearly as innovative in developing defenses as the private sector.
  - A better option might be to set up a regulatory structure that is based on performance standards instead of regulatory mandates. Under a performance standard, a company might be

given the goal of preventing, say, 95 percent of cyber attacks and left to its own devices to achieve the goal.

- To establish performance standards, the government would have to consult with the private sector to learn about existing performance requirements and develop additional sector-specific, risk-based requirements for owners of covered critical infrastructure.

- This system of guidance and standards, rather than regulatory direction, seems reasonable, but the costs of implementing performance standards may simply be too high. In the end, no one knows what standards of cybersecurity protection might be identified, and thus, no one can reasonably predict what the costs of compliance will be.

- Another criticism is that the regulatory process is too slow. Even at their fastest pace, significant government regulatory initiatives usually take at least 2 to 3 years, while the processing speed for computers doubles every 18 to 24 months. According to critics, cybersecurity standards will be out of date before they are even published.

- Finally, some technologists note that the ultra-sophisticated cyber attacks that could disable critical infrastructure will not be stopped by the adoption of best practices and standards. Thus, the regulatory solutions we are proposing won't solve the gravest problem we are trying to address.

- Jack Goldsmith, a professor at Harvard University, has noted, "Cybersecurity is an enormous challenge because most of the targets and the channels of attack are owned by the private sector, and we do not trust government regulation of the private sector, especially in the technology and communications contexts." But if not government regulation, then what?
  - One novel answer is to impose legal liability for cybersecurity failures. IT providers, such as Microsoft or Cisco, would have

to exercise a reasonable degree of care in writing code or manufacturing their products or be subject to suit.

- These companies would buy insurance to pay for damages if the suits were successful, and the insurers would, in turn, require the IT providers to meet certain standards before they were insured.

- Of course, such a change might stifle innovation, slow development, and raise prices for consumers, but it may be worth considering as an alternative to a significant government role in cybersecurity.

Suggested Reading

Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency.*

Executive Office of the President, *Cyber Space Policy Review.*

———, *Comprehensive National Cybersecurity Initiative.*

Fisher, *Creating a National Framework for Cybersecurity.*

Grady and Paris, eds., *The Law and Economics of Cybersecurity.*

Ostrom, *Governing the Commons*.

Powell, "Is Cybersecurity a Public Good?"

Rosenzweig, *Cyber Warfare*.

Thaler and Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness.*

U.S. Department of Homeland Security and National Security Agency, *Memorandum of Understanding Regarding Cybersecurity.*

Questions to Consider

1. What do you think about the question of cybersecurity regulation? Is it necessary or not?

2. If you think it is necessary, how do you think we should structure regulation to account for the rapid development of cyber technology?

3. How much would you be willing to pay in terms of increased costs for cyber access in order to be more secure? If you aren't doing anything now, why aren't you?

International Governance and the Internet

Lecture 10

Cyberspace is a domain without distinct borders, where action at a distance is the new reality. Almost every computer in America is a potential border entry point. This reality makes international engagement on cybersecurity essential. Even more notably, the sheer scale of the network demands a global approach. Who sets the rules for the Internet and what rules are set are questions that can only be answered on an international basis. This, then, is a fundamental question of cybersecurity today: How should a fractured international community respond to the phenomenon of the Internet? In this lecture, we will discuss existing Internet governance and describe some of the barriers to effectiveness in this realm.

Who Should Control the Internet?

- In the 1970s, when the Internet emerged, the various sovereign nations of the world generally ignored this innovation and let it grow with its own relatively unstructured set of governing authorities. Then, sometime around the turn of the century, sovereign nations suddenly recognized that the Internet had become an immense entity with vast influence and power.

- With that realization, sovereign nations became intensely interested in the Internet. The result is a trend toward the "re-sovereignization" of cyberspace, or what has been called the "rise of a cybered Westphalian age"—that is, an age in which sovereign nations regain control of the Internet. (The reference is to the Peace of Westphalia of 1648, which more or less defines our current system of nation-state international governance.)

- Thus, the question is: Who, if anyone, should control the Internet? Will it be separate sovereign countries? Will it be the United Nations; nongovernmental organizations, such as ICANN; or perhaps, a series of binational or multilateral groups?

- For America, this question poses a real challenge. Some think it is critical that we protect American interests and maintain our freedom of action. Others favor the development of multilateral norms to preserve the openness of the Internet, while relying on supranational organizations (such as treaty groups or the United Nations) to manage cybersecurity problems.

- The choice is of truly profound significance—perhaps more so than any other question to be addressed in the cyber domain. In one direction may lie authoritarian state control; in another, chaos. Can we perhaps find a way to maximize both security and freedom without severely compromising either?

Nongovernmental Organizations (NGOs)

- Today's Internet is controlled—to the extent anyone can be said to control it—by nongovernmental organizations (NGOs). We've already discussed ICANN, the nonprofit organization that sets the rules for creating and distributing domain names. You will recall, however, that some people do not trust ICANN.

- Another NGO, the **Internet Engineering Task Force (IETF)**, is responsible (in an indirect way) for developing the technical aspects of the computer code and protocols that drive the Internet. In other words, the actual rules for how the cyber domain works are set by the IETF, which is an "open international community of network designers, operators, vendors and researchers" concerned with the evolution of Internet architectures and the smooth operation of the Internet.

- The international régime of NGO Internet governance works pretty effectively, but there are some who doubt its neutrality. Others worry that an NGO system is a threat to nation-state power.
  - For example, despite requests from several countries, the IETF has refused to set an **encryption** standard for Internet traffic that would help governments monitor criminal (or "subversive") Internet traffic.

- This has led sovereign nations to consider ways to reassert their authority, including four non-NGO alternatives to Internet governance: isolation, international competition, multilateral agreements, and an international organization.

Isolation

- One method that some countries have chosen is isolation, that is, attempting to cut themselves off from the Internet or censor traffic arriving at their cyber borders. The most notorious example is China's attempt to construct a "Great Firewall" to keep Internet traffic out of the country.

- The instinct to regulate is not, however, limited to authoritarian régimes; even liberal Western countries, such as Australia, have proposed restrictions on Internet traffic, albeit for reasons that some people would find more legitimate, such as limiting the spread of child pornography.

- Another example of isolation comes from the relatively small nation of Belarus. In late 2011, this nation imposed restrictions on visiting and/or using foreign websites by Belarusian citizens and residents, to be enforced by its nation's Internet service providers.

International Competition

- Instead of the isolation approach, the governance of the Internet might be left to the nations of the world to sort out in competition with one another. But in this situation, the institutional interests of nation-states often lead to conflict rather than cooperation. Even Western nations sometimes disagree on the right course of action.

- The best example of this is the critical issue identified by the phrase "data sovereignty." At its core, the question here is: Whose law controls the data that are accessed and transmitted via the Internet?
  - When a customer uses cloud data storage—that is, storing data on an Internet server rather than on his or her own laptop—that customer outsources data storage requirements to a third party. The service provider owns the equipment and is responsible

for housing, running, and maintaining it. And those servers can be anywhere—in the United States, Europe, Russia, or a third-world country.

- When the customer is a private-sector company, the transition to cloud storage and processing services creates difficult jurisdictional issues. Whose law is to be applied: that of the country where the customer created the data, of the country (or several countries) where the server(s) are maintained, or of the home country where the data storage provider is headquartered?

- There is currently no international standard that governs the question of data sovereignty, nor is any institution (such as the United Nations) likely to sponsor an agreement of this nature in the near future. Rather, disputes about the control of data are resolved on a case-by-case basis, often turning on geography and/or economic factors.

- As we've said, the Internet, with its fiber optic transmission lines and server farms, has a real-world, physical presence. Every data storage facility is located somewhere. And when that "somewhere" is not in the United States, American companies (and even our government) run the risk that the data stored overseas will be subject to the sovereign control of another country.

Multilateral Agreements

- If Internet governance via international competition seems unappealing, the prospects for a multilateral response are no more promising. Consider, for example, how the multilateral impulse has begun to drive negotiations over a cyber warfare convention.
  - For years, the United States resisted Russian blandishments to begin negotiations over a cyber warfare convention akin to the chemical warfare convention. The Russian model would outlaw certain types of cyber attacks (for example, on civilian

targets, such as the electric grid). At its core, this seems a reasonable objective.

- The principal American objection has been that a cyber treaty is inherently unverifiable. Beyond verifiability, there is also a question of enforceability. There is good reason to doubt that a prohibition on targeting, say, electric grids, would be sustainable in a truly significant conflict.

- Notwithstanding these concerns, in 2009, the United States agreed to discussions with Russia and other leading cyber nations under the auspices of a group of UN experts. So far, however, little has come of those conversations. One reason for this lack of progress is that many non-Western states view the cyber domain less as a means of communication and more as a means of control—a viewpoint they want to import into any global treaty that might be adopted.

© Hemera/Thinkstock.

The United States is leading efforts to enable satellite connections to the Internet; these connections are harder to block and would allow dissidents to avoid censorship in repressive countries.

International Organization

- If the Westphalian model leads to conflict and the multilateral model involves disagreements over fundamental values, why not create an international institution to run the Internet? This option, too, is problematic.

- As we've said, the architecture of the Internet has been defined for years by two NGOs: the IETF and ICANN. Both are nonpartisan and professional, but their policymaking is highly influenced by

nations that are technologically reliant on the Internet and have contributed the most to its development and growth—in essence, liberal Western democracies. And many in the world see Western influence over the IETF and ICANN as problematic.

- The International Telecommunication Union (ITU), now a part of the United Nations, has been proposed as a better model for Internet governance. Transferring authority to the ITU (or a similar organization) is seen as a means of opening up control of the Internet into a more conventional international process that dismantles what some see as the current position of global dominance of U.S. national interests.

- Indeed, some argue that giving the ITU a role in Internet governance is no different from the role that the World Customs Organization has in setting shipping standards. To some degree that may be true, but standard shipping container sizes are not fraught with political significance in the same way that the Internet has become.
    - Such institutions as the World Customs Organization succeed precisely because they manage the mundane, technical aspects of a highly specialized industry. A similar institution would be ill-suited to provide broadly applicable content regulation for a world-girding communications system of the sort that China and some other countries would advocate.

    - It might be theoretically feasible for the ITU to restrict itself to technical questions of the sort that the IETF addresses, but even some of these questions, such as those related to encryption or content blocking, are riddled with political implications.

- At bottom, the preference for ICANN over the ITU is not just about national interests. It is also, more fundamentally, about the contrast between ICANN's general adherence to a deregulated, market-driven approach and the turgid, ineffective process of the international public regulatory sector. Recall our discussion in the last lecture about the challenges from the slow pace of the American

regulatory and policy apparatus. That problem will, if anything, be exacerbated in the international sphere.

- Thus, though there is a real intellectual appeal to the idea of an international governance system to manage the Internet, the prognosis of a cybered Westphalian age lightly controlled by NGOs is almost certainly more realistic. We are likely to see the United States make common cause with trustworthy allies and friends around the globe to establish cooperative mechanisms that yield strong standards of conduct while forgoing engagement with multilateral organizations and authoritarian sovereigns.

Important Terms

encryption: The act of concealing information by transforming it into a coded message.

Internet Engineering Task Force (IETF): A self-organized group of engineers who consider technical specifications for the Internet. The IETF sets voluntary standards for Internet engineering and identifies "best current practices." Though the organization has no enforcement mechanism, IETF standards are the default for all technical Internet requirements.

Suggested Reading

Demchak and Dombrowski, "Rise of a Cybered Westphalian Age."

Executive Office of the President, *International Strategy for Cyberspace.*

Goldsmith, "Cybersecurity Treaties."

Rosenzweig, *Cyber Warfare*.

Questions to Consider

1. Do you think that American influence on ICANN is problematic? Do you think that other countries are reasonable in having that concern?

2. Would a UN agreement on cyber weapons be verifiable? Even if it isn't, is it worth setting some norms of international behavior?

3. Should the United States resist international rules of the road for Internet governance or welcome them?

The Constitution and Cyberspace

Lecture 11

In the last two lectures, we have asked whether or not the government can and should regulate the security of the cyber domain. In this lecture, we will shift the focus slightly to a different question; instead of asking about government regulation, we will look at the idea of government control and protection. One of the goals of the Constitution is the creation of a government to "provide for the common defense." Is the federal government also responsible for defending cyberspace? Is government monitoring of the network for possible malicious activity always a good thing? In this lecture, we'll talk briefly about on-network monitoring systems and the constitutional limits of government monitoring.

Einstein

- Federal programs for on-network monitoring go by the generic name **Einstein**. Einstein 2.0 is an intrusion detection system fully deployed by the federal government in 2008 to protect federal cyber networks. A later iteration of Einstein will be moved from the federal system and deployed on private networks to protect critical infrastructure. These private networks are the same ones we all use in our online activities.

- Einstein 2.0 operates through a "look-up" system. It has a database of known malicious code signatures and constantly compares incoming messages with that database. When it finds a match, it sends an alert to the recipient. The malicious signatures are gathered from a variety of sources, including both commercial firms, such as Symantec, and government agencies, such as the National Security Agency (NSA). Einstein 2.0 is a gateway system; it screens but does not stop traffic as it arrives at federal portals.

- Einstein 3.0, the next generation of the program, is based on a classified NSA program known as Tutelage and is different in several respects.

- First, its goal is to go beyond Einstein 2.0's capabilities of detection of malware to actually prevent intrusion. To do this, Einstein 3.0 must intercept all Internet traffic bound for federal computers before it is delivered, delay it temporarily for screening, and then pass it along or quarantine the malware as appropriate.

- Second, Einstein 3.0 adopts a less definitive and more probabilistic method of identifying malware—something different from the current "look-up" system. This new system goes by the generic name of "anomaly detection." In essence, the Einstein 3.0 program knows what "normal Internet traffic" looks like and can produce an alert when the incoming traffic differs from normal by some set tolerance level.

- For this system to be effective, the Einstein 3.0 screening protocols must reside outside the federal government firewalls, on the servers of trusted Internet connections. As you might expect, for the federal government, these trusted Internet connections are all operated by American companies.

- There is little real legal debate over the operation of Einstein 3.0 as applied to government networks. Almost everyone who has examined the question agrees that it is appropriate and necessary for the government to monitor traffic to and from its own computers. Legal disagreement is much more likely to arise over how deeply a government-owned and -operated system may be inserted into private networks, to protect either the government or private-sector users. Would such a system pass constitutional muster?

Fourth Amendment Issues

- Current doctrine makes it clear that there is a difference in the level of constitutional protection between the content of a message and the non-content portions, such as the address on the outside of an envelope. In general, the non-content portions of intercepted traffic are not protected by the Fourth Amendment, which prohibits unreasonable searches and seizures.

- The Supreme Court addressed these questions in a related context in two 1970s-era cases: *United States v. Miller* and *Smith v. Maryland*. In both cases, the question was, in effect: Does an individual have any constitutional protection against the wholesale disclosure of personal information that had been collected legally by third parties? In particular, could an individual use the Fourth Amendment to prevent the government from using data it had received from a third-party collector without first getting a warrant?

© Hemera/Thinkstock.

In the 1970s, the Supreme Court determined that people cannot be, in effect, "a little bit public and a little bit private"; what you disclose to anyone is fair game for everyone.

- In both cases, the court answered with a resounding no. Along the way, it developed an interpretation of the Fourth Amendment that has come to be known as the "third-party doctrine": One has no constitutional rights to protect information voluntarily disclosed to others. The reasoning is that by disclosing information, the owner has given up any "reasonable expectation of privacy" that he or she might have had.

- In a much more recent case, *United States v. Jones*, the Supreme Court indicated that it might reconsider the third-party doctrine in light of technological changes, but it hasn't taken that step yet. Thus, we are left with the doctrine from the 1970s.
  - In the context of Internet traffic, this means that non-content header information, such as IP addresses and "to" and "from" lines, are not protected as a matter of constitutional law.

  - The *Miller/Smith* rule does not, however, permit the use of an intrusion prevention system to routinely scan the content

portions of an Internet exchange. A government program typically may not review the content portions of a message without probable cause and a warrant.

- But in the cyber realm, the line between content and non-content is not always clear. Even more significantly, the content portions of an Internet transmission may also be the portions of a message that contain malware. As a consequence, any intrusion detection or prevention system that will be of value in protecting the network must have the ability to look at the content of communications if it is to be effective.

- For Internet traffic directed to federal computers, the content/non-content distinction is comparatively easy to solve. Our Fourth Amendment concerns can be addressed by using a robust form of consent. The idea here is that protection against government scrutiny is a constitutional right, but it is a right you can give up voluntarily if you want to. If you give your consent to government screening of your e-mail, then all of the legality problems disappear.
  - Interestingly, the consent concerns are more for the recipient (some federal employee) than for the sender. As we said, the sender loses his or her privacy interest in the content of an Internet communication when it is delivered.

  - The recipient employee might have a privacy interest in the contents of an e-mail, but the government typically makes consent to e-mail monitoring a condition of employment.

The DIB Pilot

- The federal government has begun to expand this monitoring presence into the private sector, where neither the sender nor the recipient is a federal employee or agency. This extension began with voluntary agreements between the government and large government contractors in the defense industrial base (DIB). Unsurprisingly, the program is known as the DIB pilot.

- To foster their ability to do business with the federal government, these government contractors have agreed to deploy Einstein on their own systems and monitor incoming Internet traffic using government-provided threat-signature information. The decision to join the program is voluntary, but those companies that don't join will likely lose their opportunity to do business with the government.

- As with communications bound for the federal government, under the DIB pilot, the non-content addressing information is not protected by the Fourth Amendment, and the senders have no expectation of privacy. As to the actual content of a message, all of the employees of the DIB participants—such companies as Raytheon and Boeing—are asked to consent to scrutiny of their communications as a condition of employment.

- This so-called "voluntary" consent model is readily expandable to almost any industry that is dependent on federal financing and, therefore, susceptible to government pressure. Already, there is talk of extending this model to the financial and nuclear industries. A more problematic extension might be to the health-care industry or the education community.

- Even though it is probably legal to expand the federal government's protection of critical infrastructure, is it a good idea? The honest answer is that nobody yet knows. This really is an empirical question: How effective is the extended protection, and how great is the risk of abuse?
  - Although it is easy to think of theoretical answers, our policymakers are seeking hard data, and to their credit, they are doing so in a cautious way.

  - Most notably, instead of the NSA running an Einstein 4.0 program on private-sector networks, the DIB pilot program involves two limitations that are not legally necessary: First, the Einstein program is actually run by private-sector Internet service providers, and second, the private-sector DIB pilot

members are not required to provide any feedback to the NSA on the effectiveness of the program.

- This pilot has already produced two "lessons learned."
  - First, there is persistent controversy over federal involvement in cybersecurity, based in part on the argument that the private sector is generally more nimble and more knowledgeable in key respects about its own systems than the federal government could ever be.

  - Second, a fear of government intervention can have a tendency to hamstring the effectiveness of our collective approach to cybersecurity. This may not necessarily be a bad thing; sometimes, social values of independence are more important than efficiency and effectiveness.

- In mid-2012, the Department of Defense expanded the pilot, made it a permanent program, and transitioned part of its management to the Department of Homeland Security, a civilian agency thought to be better suited for long-term management of civilian cybersecurity programs. This form of consented government monitoring of critical infrastructure is likely to be part of our plan of defense for the foreseeable future.

Private-Content Network Traffic

- What about private-to-private Internet traffic that is not directed to or from a critical infrastructure industry or connected in some other way to the government? Here, the legal limits on the scrutiny of private-content network traffic are at their highest and are likely to prevail. This is not to say that the private-sector Internet is without protection, but it does mean that the American government is likely to have little if any active role in the protection of most of the Internet, both domestically and globally.

- For many in the cyber community, that is the right result. Others, however, look at this dichotomy and see a trend toward a bifurcated Internet: one portion a closed, walled garden protected by high

security, and the other, a virtual free-fire zone reminiscent of the Wild West in the mid-1800s. Neither model seems optimal, and we will no doubt continue to search for a better way.

- One reasonably safe prediction is that governments will come under increasing pressure to provide security services on the Internet. This will likely come to pass, notwithstanding the fears of a threat to civil liberties, but only with significant oversight.

Important Terms

Einstein: Intrusion detection and prevention systems operated by the federal government, principally to protect federal networks against malicious intrusions of malware.

Suggested Reading

Rosenzweig, *Cyber Warfare*.

U.S. Department of Justice, Office of Legal Counsel, "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch."

———, "Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch."

Questions to Consider

1. The third-party doctrine comes from a time when the government really didn't have the ability to systematically collect non-content data. Do you think it should be rethought in light of new technology? If so, what should it be replaced with?

2. Consent is at the core of much of our law. You consent, for example, to an airport search when you go to the airport, even though you don't have a real, practical choice. Try to think of all the places where a narrower

form of consent would change what government does. Would that be a good thing, or would it create security and law enforcement holes?

3. If you like the idea of using consent to protect our electric grid and defense manufacturing, where do you draw the line and why? Which industries should not be brought under the protective federal cyber umbrella?

Big Data—"They" Know Everything about You

Lecture 12

The film *Minority Report* portrays a world in which everything about you is known and your future actions can be predicted with accuracy. It is the world of George Orwell's *1984*, made real by advanced technology. The story is fiction, of course, but nobody is sure for how much longer. We call this phenomenon the problem of "big data." Every click you make in cyberspace can be tracked; your cell phone broadcasts your geo-location constantly; and all your purchases are cataloged somewhere. Taken together, this information can be analyzed to paint a picture of you—one that, increasingly, others can see. This lecture begins a two-part discussion of the big data phenomenon.

Defining "Big Data"

- In an increasingly networked world, personal information is widely collected and widely available. As the storehouse of data has grown, so have governmental and commercial efforts to use these personal data for their own purposes.
  - Commercial enterprises target ads and solicit new customers. Governments use the data to, for example, identify and target previously unknown terror suspects. We have discovered that we can link individual bits of data to build a picture of a person that is more detailed than the individual parts.
  - The growth in the amount of data available, married to the increase in analytical capability, is known as the phenomenon of big data.
- Clearly, big data offers all kinds of opportunities to those who have access to it. Yet this new capability also comes at a price: the peril of creating an ineradicable trove of information about innocent individuals. If the government collects data to build a picture of, say, an unknown terrorist threat, it can also use data to build a picture of its political opponents. That sort of use of cyberspace

poses threats in America and, perhaps even more frightening, in authoritarian nations abroad.

- In thinking about this capability and the opportunities and threats it presents, we sometimes talk out of both sides of our mouths. The Total Information Awareness (TIA) program, initiated by the Defense Advanced Research Projects Agency in the aftermath of September 11th, was condemned as the harbinger of Big Brother. But in other instances, the government has been criticized for its failure to perform data analysis to intercept terrorist plots.

- The conundrum arises because the analytical techniques are fundamentally similar to those used by traditional law enforcement agencies—taking a lead and finding connections—but they operate on a much larger set of data, and those data are much more readily capable of analysis and manipulation. As a result, the differences in degree tend to become differences in kind.

Big Data Drivers

- The phenomenon of big data derives from two related yet distinct trends: increases in computing power and decreases in data storage costs.

- The steady increase in the power of computers is best expressed in Moore's law, named after Intel computer scientist Gordon Moore, who first articulated the law in 1965.
    - Moore's law predicts that computer chip capacities will double every 18 to 24 months, and it has been remarkably accurate for nearly 30 years.

    - The power of this processing capacity translates almost directly into processing speed. It is what drives the IT tools that power Google and Amazon and make Walmart's purchasing system a reality.

- Although no one predicts that processing speed will double indefinitely, there is no current expectation that the limits of chip capacity have been reached.

- Married to this trend is the remarkable reduction in the costs of data storage. These costs have also been decreasing at a logarithmic rate, almost identical to the increases in chip capacity but in the other direction.
  - In 1984, it cost roughly $200 to store a megabyte of data, but by 1999, that cost had sunk to $0.75. Today, you can buy 100 megabytes of data storage capacity for $0.01.

  - In 2009, the entire Internet was roughly 500 exabytes (an exabyte is 1 billion gigabytes), yet within 10 years or so, that storage capacity may be available to a small corporation. We can hardly imagine what a large corporation or a government could maintain.

Practical Obscurity

- Our law and policy thinking has not yet caught up with the reality of ever-quicker processing power and ever-cheaper storage capacity. Ten years ago, surveying the technology of the time, Scott McNealy, then-CEO of Sun Microsystems, said, "Privacy is dead. Get over it."
  - What he was describing was the loss of public anonymity—the ability to act (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data about your activity for later analysis.

  - American law has a phrase to describe this phenomenon: "practical obscurity." Derived from a 1989 Supreme Court case, *Department of Justice v. Reporters Committee*, the origin of the phrase is instructive in illuminating the effects of the change in technology.

- In the late 1980s, the Department of Justice created a database with information about the criminal records of known offenders, which until that time had been widely scattered in unconnected systems.
    - All the records were generally public, but they were dispersed among so many data-holders that no one entity could find all the information and create a comprehensive dossier on any individual. The records were "practically obscure."

    - Despite the fact that the records were public when found in disparate databases, the Justice Department denied a request from the press for collated dossiers on certain alleged Mafia figures.

    - The department's denial was later upheld by the Supreme Court, according to which, there is a "vast difference between the public records that might be found after a diligent search … and a computerized summary located in a single clearinghouse of information." Because of that difference, the court concluded that the "privacy interest in maintaining the practical obscurity of rap-sheet information will always be high."

- Today, the court's confident assertion that obscurity will "always" be high has proven to have a half-life of less than 20 years. Large data collection and aggregation companies hire retirees to harvest public records from government databases. These companies typically hold birth records, credit and conviction reports, records of real estate transactions and liens, bridal registries, and even kennel club records.

- Given that most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what it cannot create itself, it can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual.

Knowledge Discovery

- These systems of data analysis are remarkably sophisticated. They are, in the end, an attempt to sift through large quantities of personal information to identify subjects whose identities are not already known.
  - In the commercial context, these individuals are called "potential customers." In the terrorism context, they are often called "clean skins," individuals who are dangerous because nothing is known of their predilections.
  - For precisely this reason, this form of data analysis is sometimes called "knowledge discovery," because the intention is to discover something previously unknown about an individual or group of individuals.
- The events of September 11, 2001, are probably the best known example of the failure of knowledge discovery, that is, the government's inability to use big data to "connect the dots." As a Department of Defense review committee later concluded, all 19 of the terrorists involved in the September 11 attacks could have been easily identified and linked through existing public databases.

More than 350 million people cross American borders each year; the Department of Homeland Security uses the Automated Targeting System to identify some of those travelers for more intense scrutiny.

- The story of Ra'ed al-Banna, a Jordanian who attempted to enter the United States at Chicago's O'Hare Airport on June 14, 2003, is a powerful illustration of the successful use of big data. Al-Banna was probably a clean skin, but he was flagged by the Department of Homeland Security's Automated Targeting System and denied entry to the United States. More than a year later, al-Banna was responsible for a car bombing in Iraq that killed more than 125 people.

The Personal Power of Big Data

- A chart compiled by David McCandless, a London-based data journalist, showing Facebook data relating to the breaking up of romantic relationships represents the kind of pattern we would not see without big data. Depending on your point of view, this level of knowledge discovery may be exciting or disturbing.

- A free program called Collusion, an add-on for Firefox, allows you to track how your browsing habits are being collected. You may not realize that your visit to a particular website is shared with numerous other websites. The sites collude, in other words, to build a better picture of who you are.

- Again, depending on the context, what might seem only a bit creepy can become pretty scary and downright authoritarian.
    - For example, your cell phone is constantly reporting your location to the nearest cell towers. That's how the system knows where you are so that it can connect a call to you.

    - But your phone company keeps those records of where your cell phone is, which means that it knows where you are and where you've been. A six-month log of your travel might reveal whether you are a churchgoer or a gym fanatic, or whether you visit local porn shops.

    - Perhaps you're not worried that your phone company has this information about you, but what if the company sells the

information to some commercial advertiser? Or what if the government issues a subpoena and collects all these records?

- This issue is highly contentious right now, but at the present time, the *Miller/Smith* third-party doctrine applies. That's the doctrine that says that information you share with a third party, such as Facebook or your phone service provider, is not protected by the Fourth Amendment. That means that you have no privacy interest in the location data that you "voluntarily" broadcast to the cell phone company.

Suggested Reading

Bailey, *The Open Society Paradox.*

Harris, *The Watchers*.

Markle Foundation, *Protecting America's Freedom in the Information Age*.

———, *Creating a Trusted Network for Homeland Security.*

O'Harrow, *No Place to Hide.*

Rosenzweig, *Cyber Warfare*.

Smith, *Risk Revolution*.

Questions to Consider

1. Big data is a powerful tool for security but also for intrusions into civil liberties. Are there any ways in which we can get the benefit of it without experiencing the harm?

2. Do you think a set of laws trying to prohibit big data analytics would be successful? Why or why not?

3. Which concerns you more, the use of data analytics by the government or the commercial sector?

Privacy for the Cyber Age

Lecture 13

As we saw in the last lecture, it seems as if our new technologies are engaging in ever-expanding data collection and analysis. In the end, we might think that our current conceptions of privacy will inevitably be eroded if not destroyed. What can we do about this situation? In this lecture, we'll look at where our privacy laws come from and how we might think of changing those privacy laws, without being complete Luddites about the new technology. We will break this discussion into two parts, looking at both government's and the private sector's use of big data. We'll then close with a related topic: how big data analysis can be used to keep the government honest.

Outdated Privacy Laws

- As we saw in the last lecture, the third-party doctrine was developed by the Supreme Court in the 1970s. According to this doctrine, information disclosed to a third party is not protected by the Fourth Amendment. In the context of data privacy, this means that there is no constitutional protection against the collection and aggregation of cyber data for purposes of data analysis and to pierce the veil of anonymity.

- There is some hope that the status quo might change. In the 2012 case *United States v. Jones*, the Supreme Court gave some indication that it is thinking hard about how the standard Fourth Amendment analysis applies in the era of big data.

- For now, officially, the court and the Constitution are still on the sidelines. All that is left to preserve anonymity from government intrusion are the statutory protections created at the federal level by Congress. But those, too, are out of date.
    - Our concepts of privacy are embedded in a set of principles known as the Fair Information Practice Principles, which were

first developed in the early 1970s and have now become the keystone of the Privacy Act of 1974.

- Essentially, the principles say that the government should limit the collection of personal information to what is necessary, use it only for specific and limited purposes, be transparent and open with the public in how the information is collected and used, and allow the individual about whom the data are collected to see and correct the collected data, if necessary.

- As you can probably surmise, the technology of big data collection and analysis destroys these types of rules. A conscientious and fair application of these principles is, in many ways, fundamentally inconsistent with the way in which personal information is often used in the context of counterterrorism, or, for that matter, commercial data analysis.

- In our modern world of widely distributed networks, with massive data storage and computational capacity, so much analysis becomes possible that the old principles no longer fit. What is needed, then, is a modernized conception of privacy—one with the flexibility to allow effective government action but with the surety necessary to protect against government abuse.

A New Definition of Privacy

- The first step in developing a new legal structure to fit with changing technology is to dig deep into the idea of privacy. This term reflects a desire for independence of personal activity, a form of autonomy.

- We protect privacy in many ways. Sometimes, we do so through secrecy, obscuring both the observation of conduct and the identity of those engaging in the conduct. An example of this might be the voting booth, where who you are and what you do are both obscured behind a screen to create a secret environment.

- In other instances, we protect autonomy directly, as, for example, when we talk about privacy rights in connection with freedom of

religion or the right to marry whom you choose. Indeed, the whole point of that kind of privacy is to allow people to act as they wish in public—which is a bit of an odd idea of privacy.

The concept of privacy that most applies in our technological age is the idea of anonymity, similar to what we expect when driving a car: We drive in public, but we aren't subject to routine scrutiny when driving.

- The concept of privacy that most applies to the new information technology regime and the use of big data is the idea of anonymity. It's a kind of middle ground where observation is permitted—that is, we expose our actions in public—but where our identities and intentions are not ordinarily subject to close scrutiny.
    - The information data space is, as we've seen, suffused with information of this middle-ground sort: bank account transactions, phone records, airplane reservations, and so on. They constitute the core of the transactions and electronic signature or verification information available in cyberspace.

    - The type of anonymity that one must respect in these transactions is not terribly different from "real-world anonymity." Consider, as an example, the act of driving a car. It is done in public, but one is generally not subject to routine identification and scrutiny in performing the act.

- Protecting the anonymity we value requires, in the first instance, defining it accurately. One might posit that anonymity is, in effect, the ability to walk through the world unexamined. That is, however, not strictly accurate, because our conduct is examined numerous

times every day. Thus, what we really mean by anonymity is not a pure form of privacy akin to secrecy.

- Rather, our definition should account for the fact that even though our conduct is routinely examined, both with and without our knowledge, nothing adverse should happen to us from this examination without good cause. The veil of anonymity—previously protected by "practical obscurity"—is now readily pierced by technology. Instead of relying on the lack of technical ability to protect privacy, the veil must be protected by rules that limit when piercing is allowed.

- To put it more precisely, the key to this conception of privacy is that privacy's principal virtue is a limitation on consequence. If there are no unjustified consequences—that is, consequences that are the product of abuse, error, or the application of an unwise policy—then under this vision, there is no effect on a cognizable liberty/privacy interest. In effect, if nobody is there to hear the tree or identify the actor, it really does not make a sound.

- In the government context, the questions to be asked of any data analysis program are: What is the consequence of identification? What is the trigger for that consequence? Who decides when the trigger is met? These questions are the ones that really matter, and questions of collection limitation or purpose limitation, for example, are rightly seen as distractions from the main point.

Protecting Privacy

- Using this new working definition, how do we protect privacy and its essential component of anonymity? The traditional way is with a system of rules and oversight for compliance with those rules. Here, too, modifications need to be made in light of technological change.

- Rules, for example, tend to be static and unchanging and do not account readily for changes in technology. Indeed, the Privacy Act is emblematic of this problem; its principles are ill-suited to

most of the new technological methodologies. Thus, we have begun to develop new systems and structures to replace the old privacy systems.

- First, we are changing from a top-down process of command-and-control rule to one in which the principal means of privacy protection is through institutional oversight. To that end, the Department of Homeland Security was created with a statutorily required privacy officer (and another officer for civil rights and civil liberties). Later legislation has gone even further, creating a civil liberties protection officer within the intelligence community and an independent oversight board for intelligence activities.

- These offices act as internal watchdogs for privacy concerns and serve as a focus for external complaints that require them to exercise some of the functions of ombudsmen. In either capacity, they are in a position to influence and change how the government approaches the privacy of its citizens.

- Finally, and perhaps most significantly, the same systems that are used to advance our government's interests are equally well suited to ensure that government officials comply with the limitations imposed on them in respect of individual privacy. The data analysis systems are uniquely well-equipped to "watch the watchers," and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others.

- If we do these three things—reconfigure our conception of privacy, put the right control systems in place, and use a strong audit system for the government—we could be reasonably confident that a consequence-based system of privacy protection would move us toward a place where real legal protections could be maintained.

Commercial Data Collection

- The collection of private data in the commercial sector presents a different set of challenges.

- On the one hand, the Constitution doesn't apply to private commercial actors, so that's not a potential avenue for protecting privacy.

- On the other hand, the field is wide open for Congress to regulate in this area. Unlike government data mining, where the purpose is at least theoretically to protect national security, there is no urgent interest in commercial data mining. Thus, when Congress steps in to limit it, the only negative consequence is that some settled commercial expectations may be upset.

- We should not, however, downplay the costs involved with that kind of interference in the market. At this point, the value of commercial use of big data has become so deeply embedded in the business model of cyberspace that it would be difficult to modify.

- The commercial arena is already moving toward a system that resembles the "consequence" idea of privacy that we have discussed. In the future, we will almost certainly have a "Do Not Track" rule for data similar to the "Do Not Call" list to avoid telemarketers.

The Flip Side of Privacy: Transparency

- The flip side of the loss of privacy may be a gain in transparency, especially in the realm of government action. The identification of a team of Israeli assassins by law enforcement authorities in Dubai vividly illustrates the idea that governments—just like citizens—are losing their privacy.

- Technological development has complicated the job of intelligence agencies in conducting undercover operations. Too many trails in cyberspace can provide evidence that a false identity is a recent creation. Indeed, we may well be reaching the point where human spying with a fictitious identity is a thing of the past. Although

governments might consider this a problem, some people might think it's a good thing.

- The phenomenon of big data is here to stay, and determining the right answers to many of the questions posed in this lecture will be a significant challenge. We will likely have different answers depending on the context. Instead of opposing technological change, a wiser strategy is to accept it and work to channel it in beneficial ways.

Suggested Reading

American Bar Association, Office of the National Counterintelligence Executive, and National Strategy Forum, *No More Secrets*.

Bailey, *The Open Society Paradox.*

Harris, *The Watchers*.

Markle Foundation, *Protecting America's Freedom in the Information Age*.

———, *Creating a Trusted Network for Homeland Security.*

Mayer-Schoenberger, *Delete: The Virtue of Forgetting in the Digital Age.*

O'Harrow, *No Place to Hide.*

Raul, *Privacy and the Digital State*.

Rosen, *The Naked Crowd*.

Rosenzweig, *Cyber Warfare*.

Smith, *Risk Revolution*.

Solove and Schwartz. *Privacy, Information and Technology.*

Questions to Consider

1. Is government transparency always a good thing? Are there some secrets the government should be able to keep?

2. Do you agree that we need a new way of thinking about privacy? If you do, how would you define it? Or do you think that the old rules work just fine and don't need to change?

3. One problem with thinking about privacy as focused on consequence is that some people think that individuals change their behavior just because they know (or think) they are being watched, even if nothing happens. Do you agree? If you do, can you think of any way to protect against observation in a big data world?

Listening In and Going Dark

Lecture 14

As communications technology moves to cyberspace, law enforcement and national security officials are becoming frustrated. The messages that travel through cyberspace are encrypted and broken up into packets, so they can't be intercepted. This "going dark" problem means that our law enforcement agents are losing the ability to listen in on the conversations of criminals, terrorists, and spies. In this lecture, we'll look at two issues that relate to the security of cyber communications: encryption and wiretapping. Technological developments in these two areas have led to controversy over critical cybersecurity policy issues. Can a government require code makers to build in a "back door" to allow access to, and decryption of, encrypted messages?

Traditional Encryption

- Conceptually, encryption involves three separate components: the plaintext, algorithm, and key.
  - The plaintext is the substance of the message that the sender wants to convey. Of course, this information doesn't have to be a text at all; it can be the numerical firing code for a nuclear missile or the formula for Coca-Cola products.

  - The algorithm is a general system of encryption, that is, a general set of rules for transforming a plaintext. An example of an algorithm is a cipher in which, say, each letter of the plaintext is replaced with another letter. The algorithm here would be: "Replace each letter with another."

  - The third and most vital component of an encryption system is the key, that is, the specific set of instructions that will be used to apply the algorithm to a particular message. A cipher key might be: "Replace the original letter with the letter that is five letters after it in the English alphabet." The result would be known as the ciphertext.

- The critical feature, of course, is that as an initial premise, only someone who has the algorithm and the key can decrypt the ciphertext; thus, even if the ciphertext is physically intercepted, the contents remain confidential.

- It is one of the truisms of encryption that the "key" to keeping a secret is the key—not the algorithm. The algorithm—the general method—is often too widely known to be usefully kept secret. Thus, the strength of the key—how hard it is to guess—defines how good the encryption product is.

- Since at least the 9th century, it has been well-established that a cipher can be broken by frequency analysis rather than brute force.
  - Frequency analysis rests on the knowledge that, for example, in English, the letter *e* is the most common vowel. Other common letters in regular usage include *a*, *i*, *n*, *o*, and *t*.

  - With this knowledge derived from analysis external to the code, the deciphering of a ciphertext is made much easier. It is far more likely than not that the most frequently used cipher letter, whatever it may be, represents one of these common English letters. In a ciphertext of any reasonable length, there is virtually no chance, for example, that the most common cipher letter is being used to signify a *q* or a *z*.

  - This sort of knowledge makes decryption easier and reduces the need for a brute force approach. Indeed, it is a fair assessment of the art of cryptography that, until the dawn of the computer era, those decrypting ciphers had the upper hand. Either the keys themselves could be stolen, or they could be decrypted using sophisticated techniques, such as frequency analysis.

Modern Encryption

- In the late 1970s, a method of encryption was developed using the multiplication of two extremely large prime numbers and certain one-way mathematical functions. With one-way functions, someone who wants to receive encrypted messages can publish the result of

an extremely large multiplication as a public key. People who want to send this person a message can use the public key to encrypt their messages, but only the creator knows how to break the large number into its original primes; thus, only the creator can decrypt the message.

- Today, this type of encryption can be embedded into your e-mail system using a program that can be purchased over the Internet for less than $100. If the users at both ends of a message use this form of public key encryption, the secret message they exchange becomes, effectively, undecryptable by anyone other than the key's creator—unless, of course, a hacker attacks the creation of the key at its source, by breaking into the key-generation algorithm.

- This last scenario was thought to be entirely theoretical: Nobody could break into the key-generation process—until someone (probably the Chinese) did in March 2011, hacking into a company named RSA, the leading manufacturer of public encryption key devices.

Key Escrow

- The U.S. government has suggested a system of "key escrow" to enable it to carry out its law enforcement responsibilities. Under this system, those who manufacture encryption software would be required to build in a back-door decryption key that would be stored with a trusted third party, perhaps a judge at a federal court. The key would be released only under specified, limited circumstances.

- Needless to say, many privacy advocates opposed this effort, and their opposition was successful. In the 1990s, the FBI sought to require encryption technology manufacturers to include such a back door that went by the name of "Clipper chip." Opposition to the program on a number of fronts resulted in its demise.

- At this juncture, encryption technology is widely available, with exceedingly strong encryption keys. In effect, with the death of the

Clipper chip back-door movement, it is now possible to encrypt data in a way that cannot be decrypted after even a year of effort.

Wiretapping

- Just as changes in cyber technology have made encryption a reality, they have also come close to ending the practice of **wiretapping**. Pre-Internet, wiretapping was an easy physical task. All that was required was attaching a wire to a terminal post and then hooking the connection up to a tape recorder. The interception didn't even need to be made at the central public switched telephone network (PSTN); any place on the line would do.

© iStockphoto/Thinkstock.

Early telephony worked by connecting two people who wished to communicate through a single, continuous wire; this system made wiretapping an easy matter.

- Today, the problem is more complex; we have created an almost infinite number of ways in which we can communicate. When combined with the packet-switching nature of Internet web transmissions and the development of **peer-to-peer** networks (networks that completely eliminate centralized servers), the centralized telephone network has become a dodo. With these changes, the laws and policies for authorized wiretapping have, effectively, become obsolete.

Legal and Technical Challenges

- The law enforcement and intelligence communities face two challenges in administering wiretap laws in the age of the

Internet: one of law and one of technology. The legal issue is relatively benign and, in some ways, unencumbered by technical complexity. We need a series of laws that define when and under what circumstances the government may lawfully intercept a communication. The technical issue is far harder to solve: Precisely how can the desired wiretap be achieved?

- In 1994, Congress attempted to address the legal problem through the Communications Assistance for Law Enforcement Act (CALEA).
  - CALEA's purpose was to ensure that law enforcement and intelligence agencies would not be left behind the technology curve. It did so by requiring telecommunications providers to build the ability to intercept communications into their evolving communications systems.

  - Thus, the providers of the then-new digital technologies of cell phones and e-mail services were required to create a way of intercepting these new forms of communication that would be made available to law enforcement if a warrant was issued. But that was a generation ago—an eternity in cyber time.

  - Unsurprisingly, as technology has moved forward, the law has not kept pace. Nothing today requires the manufacturers of new communications technologies to have similar capabilities. Quite literally, for some systems, even if a lawful order were forthcoming from a court, there would be no place in the system to hook in the figurative alligator clips and intercept the communication.

  - This means that cyber criminals, cyber spies, and cyber warriors are increasingly migrating to alternative communications systems—Skype and virtual worlds that are completely disconnected from the traditional PSTNs and even from the centralized e-mail systems operated by such companies as Google. And as we've already discussed, the distributed

nature of communication via these systems makes message interception extremely difficult.

- To compensate, the government must use sampling techniques to intercept portions of a message, and then, when a problematic message fragment is encountered, apply sophisticated methods to reassemble the entire message. Often, the reassembly is achieved by arranging for the whole message to be redirected to a government endpoint.
  - The FBI developed such a system in the late 1990s, called Carnivore. It was designed to "sniff" packets of information for targeted messages. When the Carnivore program became public, the uproar over this sort of interception technique forced the FBI to end it.
  - It is said that the NSA uses a packet-sniffing system called Echelon that is significantly more effective for intercepting foreign communications traffic than Carnivore ever was.
  - In order for such a system to work, however, the routing system must ensure either that traffic is routed to the sniffer or that the sniffer is physically located between the two endpoints. But therein lies the problem: Many of the peer-to-peer systems are not configured to permit routing traffic to law enforcement sniffers.
  - To address these problems, the U.S. government has spoken publicly of its intent to seek an amendment to CALEA, although such an amendment would not put an end to legal questions.
- Finally, we need to recognize that the issues raised by the government's push for greater wiretapping authority are more policy questions than legal questions. What would be the security implications of requiring interception capabilities in new technologies? And how would granting the U.S.

government the access it wants affect international perceptions of American conduct?

- Encryption and wiretapping capabilities are yet another example of the type of problem we've come to expect in the cyber domain. They bring benefits and cause problems, and any solution brings with it problems of its own. In the end, we will probably see some increased government access to unencrypted Internet communications, but at least in the United States, only under the control of the courts.

Suggested Reading

peer-to-peer: Most Internet transmissions involve some routing by intermediate servers that serve a controlling function. Peer-to-peer systems, as the name implies, enable direct communications between two (or more) endpoints without the need for intermediate routing and with no centralized or privileged intermediary.

wiretapping: The interception of a message in transit by someone who is not the intended recipient. The term comes from the practice of attaching two clips to a copper telephone wire to intercept a phone call.

Important Terms

Al-Kadi, "The Origins of Cryptology."

Gardner, "A New Kind of Cipher That Would Take Millions of Years to Break."

Landau, *Surveillance or Security*.

Levy, *Crypto*.

Rosenzweig, *Cyber Warfare*.

Singh, *The Code Book.*

Questions to Consider

1. Do you think the U.S. government should ever have access to Internet communications? If you do, what rules do you think should apply to limit when that access is permitted?

2. Do you have an encryption system on your own home computer? If not, why not?

3. If American companies were required to have back doors in their systems, would you buy them? Do you think you would even know they were present?

The Devil in the Chips—Hardware Failures

Lecture 15

In testimony before the House of Representatives in July 2011, the Department of Homeland Security confirmed that it was aware of situations where electronic equipment had arrived preloaded with malware, spyware, or other forms of hardware intrusion. This is now one of the most vexing problems in the domain of cybersecurity. Cyber threats can lurk not only in computer software but also within the various routers, switches, operating systems, and peripherals that comprise the real-world manifestations of cyberspace. In this lecture, we'll explore the question: How do we know that the machines we are using will actually do the things we tell them to and not something else that could be harmful?

Supply-Chain Attacks

- Over the past decades, the U.S. government has become increasingly reliant on commercial off-the-shelf (COTS) technology for much of its cyber supply needs. Indeed, counterterrorism experts have sometimes said that American reliance on COTS computer technology, which is often manufactured or maintained overseas, poses a greater vulnerability to U.S. cyber systems than traditional cyber attacks.

- This new, hardware-based form of espionage is completely different from regular spying, and we have no good systems in place to counter threats that are inside our machines.

- This troubling new activity is actually an attack on our supply chain. An adversary might get into our communications system by subverting the manufacturing process long before the product that will be added to the system makes it to our shores. We call this an "assurance" problem because we need to assure ourselves that the hardware works.

- The **Cyberspace Policy Review** conducted by President Obama early in his administration put the problem this way: "The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover."

- In 2010, the **Comprehensive National Cybersecurity Initiative (CNCI)** identified "global supply chain risk management" as one of the initiatives critical to enhanced cybersecurity, yet the United States has a very limited set of systems in place to respond to this challenge.
  - Indeed, there is a disconnect between our counterintelligence, which is often aware of risks to our cyber supply chain, and our purchasing systems, which do not have permission to access classified information regarding supply-chain threats.

  - Setting aside intelligence concerns, the idea of creating a blacklist of unacceptable products for purchase is fraught with problematic issues regarding liability and accuracy.

  - Even if we could devise a means of giving the procurement process access to sufficient information and even if liability issues could be overcome, it might well be the case that no significant alternative sources of supply exist. We are dependent on foreign chips in the same way, for example, that we are dependent on foreign supplies of rare earth metals and, to a lesser degree, oil.

- Nor is the problem limited to the government. As evidenced by the examples involving Android mobile phones, Barnes & Noble, and AT&T, it applies to private-sector systems, too.

Scope of the Problem

- Today, more than 97 percent of silicon chips (the essential innards of the computer) are manufactured outside the United States. Each chip has more than 1 billion transistors. In 2008, the world manufactured 10 quintillion transistors.

- There is no way to inspect all the transistors and chips that are manufactured and incorporated in our computers (and copiers, printers, and so on). And even if there were, or if we were able to sample them randomly somehow, there is also no effective way to detect when a chip has been deliberately modified.

- Given that we can't solve the problem from the bottom up by inspecting the chips, the only way to look at the problem is from the top down and ask what we know about who is making the chips we rely on. At present, there are only two structures in operation within the U.S. government that provide a means of addressing supply-chain security issues, and neither is particularly adept or well-suited to the task.
    - One is the Committee on Foreign Investment in the United States (CFIUS), an interagency committee authorized to review transactions that could result in control of a U.S. business by a foreign company. CFIUS was initially created to focus on the sale of companies that would result in foreign control of defense-critical industries; it now also focuses on sales that will affect critical infrastructure.

    - The other organization is the Federal Communications Commission (FCC). Whenever it has concerns about the purchase of an interest in an American telecommunications company, the FCC refers those questions to an interagency working group that reviews the transaction to determine whether there might be a national security concern.

    - These are very limited tools, and they only apply when a foreign company plans to purchase control of an American one. If the American company simply purchases a product from overseas, there is absolutely no way, currently, for anyone in the government to do more than express concern.

Reliance on COTS Technologies

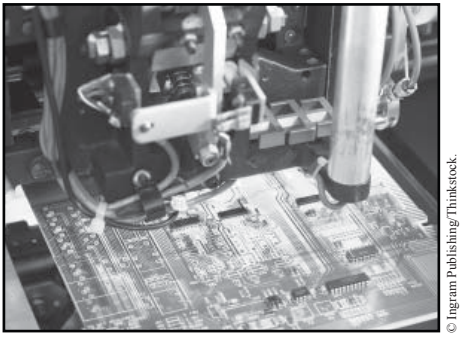
- Counterintelligence experts find the internal hardware threat more challenging than the potential for an external cyber attack.

The globalization of production for both hardware and software makes it virtually impossible to provide either supply-chain or product assurance.

- The vulnerability is made acute by the fact that the U.S. government and the private sector have come to rely on COTS technologies, which have many obvious advantages.
  - They are generally cheaper than custom-built solutions, and because they are produced in the private sector, they are modified and upgraded more rapidly, in a manner that is far more consistent with the current technology life cycle.
  - Particularly in the cyber realm, where upgrades occur with increasing frequency, reliance on COTS technology allows government and the private sector to field the most modern equipment possible.

- However, in moving away from custom solutions, U.S. government systems have become vulnerable to the same types of attacks as commercial systems. The vulnerabilities that come from running commercial operating systems on most government computers would not exist in the same way if our computers operated on a noncommercial system.

- This same phenomenon occurs in our hardware purchases. COTS systems have an open-architecture design; in other words, the hardware is compatible with the equipment from many different manufacturers. But



Quality control and security processes at a U.S. manufacturer attempt to negate the threat that an insider will insert malicious hardware or code into a system; the same is not necessarily true of manufacturers in other countries.

because the COTS systems are open to hardware additions, few of them have good security. Worse yet, knowledge of the design of the systems and their manufacture is increasingly outsourced to overseas production.

- There is no clear way to deal with these vulnerabilities. It is unlikely that the U.S. government and private sector will return to a time when all systems were "made in the USA." Doing so would be prohibitively expensive and would forego a substantial fraction of the economic benefits to be derived from the globalization of the world's economy. Even such a response would not eliminate the COTS problem because hardware constructed in the United States could still be built with malicious intent .

- Further, the risk is not just from hardware but also the many service functions that are purchased from foreign providers. Such service functions include product helplines, as well as repair and maintenance services.

Intelligence Collection as a Possible Solution

- One possible answer to the COTS problem might be better intelligence collection, and indeed, the government may already have some information about potential hardware intrusions. Unfortunately, the complexity of getting that information to American manufacturers and consumers has, so far, prevented effective action.

- The problem here is both a legal and a practical one. For one thing, certain issues always arise when we consider disclosing the results of the government's intelligence analysis. We risk revealing our own sources and methods. In addition, although the government may be in a position to say that the risk from a certain purchase is high, there are no guarantees, and that creates ambiguity for the private sector and procurement officers.

- Under current law, the government cannot provide information about suppliers to private companies. In addition, such an effort would create numerous potential liability questions: How certain is the government of its suspicions? How often must such an assessment be updated or modified?

- In short, the intelligence community can and does share concerns about such issues as hardware intrusions within the U.S. government, but it is legally disabled from sharing the same information with critical private-sector stakeholders.

Other Solutions to the Hardware Threat

- To date, strategies to eliminate the risk of hardware intrusions are nonexistent, and those required to mitigate it seem to be mostly nibbling around the edges. The Defense Science Board, for example, recommends that we figure out which missions and systems are most critical and focus our efforts on them, leaving others to fend for themselves. That seems a bit like accepting defeat from the outset.

- The board also recommends that purchasers investigate their suppliers. Who owns the suppliers, and how trustworthy are they? What security measures do they have in place? These are questions that need to be asked. The answers may not eliminate the risk, but we can certainly start making judgments about whom to trust.

- Additional steps we might consider include the following: (1) expanding governmental review authority to include situations in which foreign entities take control of service activities that affect the cyber domain or where foreign influence is achieved without purchasing full control; (2) diversifying the types of hardware and software systems that are used in the federal government; (3) strictly enforcing antitrust laws to compel the private sector to diversify its own operating systems; and (4) evaluating the security of products provided by suppliers.

- The hard truth is discomfiting. For as long as the purchase of hardware products occurs on the global market, there will be a significant risk of hardware intrusion. That risk can never be eliminated. It can only be managed and reduced.

Important Terms

Comprehensive National Cybersecurity Initiative (CNCI): The broad federal strategy for fostering cybersecurity in America. When first drafted in 2008, it was classified. An unclassified version was publicly released in 2010.

Cyberspace Policy Review: In May 2009, one of the first actions of the Obama administration was the development and release of a broad-based cyberspace policy review. This review has guided federal strategy since then.

Suggested Reading

Defense Science Board, *Mission Impact of Foreign Influence on DoD Software.*

Rosenzweig, *Cyber Warfare*.

U.S. Department of Commerce, *Defense Industrial Base Assessment*.

Questions to Consider

1. Should the United States begin a program of rebuilding its domestic chip manufacturing capability? That would cost quite a bit. How much would you be willing to pay for safer chips?

2. The United States is focused on a hardware threat from China and, in particular, two companies, Huawei and ZTE. What could those companies do to make us believe their chips are safe?

3. Is China the only country to be concerned about? What about manufacturing in Malaysia, Indonesia, or India?

Protecting Yourself in Cyberspace

Lecture 16

By this point in the course, you're probably completely dismayed. The Constitution doesn't protect you, big data can expose your secrets, and you can't even trust the chips in your computer to work properly. But the truth is that you can protect yourself to a much greater degree than you probably do. You don't have to become perfectly invulnerable to protect yourself in cyberspace. The only real way to do that is to use your computer as a paperweight, but that seems like an extreme solution. What you really need to do is a better job of reducing your own risks. If you improve your own security enough, the bad guys will go looking for an easier mark.

Behavioral Changes

- To begin with, a few simple changes in how you behave can go a long way to making you safer. Almost all of the vulnerabilities in a network are exploited through human error. Kevin Mitnick, one of the most infamous hackers of all time, has said, "There is no Microsoft patch for stupidity or, rather, gullibility."

- One good rule of thumb to keep in mind is this: If it seems too good to be true, it almost certainly is. Don't plug in the thumb drive you find in a parking lot. Don't click on the link to see your favorite celebrity in a compromising photo.

- In the aftermath of a natural disaster, people often set up websites to collect money and goods to help victims, but a significant fraction of those sites are frauds. If you want to give money to people in need, don't click on links in e-mails that come to your in-box; instead, choose known websites, such as that of the American Red Cross.

- Likewise, most of the official-looking e-mails you receive from your service providers or your bank are fake. If Google sends you an e-mail saying that you need to log in to your account because it

may have been hacked, don't click on the link in the message; that's the link that hacks your account!

- Finally, take a minute to turn off the "auto run" function on your computer. That way, if you do click on a dangerous link, the invading programs that are inside it won't start running automatically.

Passwords

- Resist the temptation to use easy passwords. These days, cunningly designed computer programs troll the web for vulnerable accounts. Most password-cracking programs have a huge dictionary of the top 500,000 passwords, and they simply check those first. If your password is on the list, your accounts can be hacked.

- The most common password of all is "password," and the second most common is "123456." Don't use those, and don't use obvious personal information, such as your birthday, or common cultural reference points, such as "Frodo" or "BruceSpringsteen."

- Consider using a password safe, that is, a program where you store all your passwords to various websites and accounts. Then, you protect that one program with a strong master password. Two such programs are Identity Safe and LastPass.

- Here's one system for creating a strong password: Think of your favorite line from a movie, play, or book, and make a password from the first letter of the first 10 or 15 words in that line. Then, vary the capitalization (say, every third letter is capitalized) and add in some numbers, such as the last four digits of your home phone number when you were a child.

- For the passwords you use on websites and store in your vault, don't use the same password that you use as your master password. You don't want anyone to be able to find that all-important password in more than one place. In fact, don't make a habit of reusing passwords. Have several different ones for different types

of websites. And always use a different password at work than you do at home.

- If the information you're trying to protect is really important, consider using a password alternative, such as a fingerprint scanner or a security token. Those options are expensive, but if you have a new patent coming out, you might want to protect your investment.

Firewalls and Intrusion Detection Systems

- The most effective attacks on a network often come as e-mails or files that look very much like the real thing—perhaps a corporate recruitment plan or a directory document. The best way to prevent those sorts of intrusions is to make sure you have an effective set of firewall and **intrusion detection systems** and keep them up to date.

- Some people think they don't need a computer security system because the operating system they are using is immune. That's a frequent misconception of Apple users. Apple products are targeted less frequently because fewer people use them, but as they become more widely used, hackers are having increasing success in attacking the Apple operating system.

- Mobile devices are also not immune. In fact, their protections are often weaker than those of laptops, precisely because they have been less frequently targeted. Like your laptop, your mobile device can be turned into a microphone by an outsider. The only sure way to defeat such an attack is to take the battery out of your phone or leave it outside the meeting room.

Encryption

- Another valuable way to protect your information is with encryption. As you'll recall from Lecture 14, encryption effectively turns your data into a secret code that nobody else can read without a key, solving numerous security problems in one stroke. One good free program for this purpose is TrueCrypt.

- An encryption program creates an encrypted portion of your hard drive, where you can store sensitive data. The best ones use an interface that makes this encrypted segment look just like a directory drive in your Windows or Apple system. Basically, you open up this encrypted drive space and then drag and drop your data (a Word document, an Excel spreadsheet, a photo, or the data file for your Quicken program) into the encrypted drive space. When you close the drive, all the data become an unreadable ciphertext that can be decrypted only if you have the encryption key.

- Of course, to reopen the encrypted drive, you need a password that serves as your encryption key. In the end, if you use a virtual encryption program on your hard drive, the data are accessible only to you.

Deleting Data

- The flip side of keeping your data safe is that when you delete information, you need to make sure it is truly gone. Many of us delete files by moving the icon to the recycle bin or, on Apple computers, the trash can. This does not really erase the data.

- When you move a file to the recycle bin, all you've done is erase the pointer in the directory that tells the program (say, Microsoft Word) where to go to pull up the file.
  - This is a bit like throwing out the table of contents of a book; if you still have the rest of the book, you can find the chapter you're looking for, even without a table of contents.

  - Likewise, an intruder in your system who has access to your entire hard drive and is seeking to steal some intellectual property doesn't really need to know where the files are. It helps, of course, but with a little bit of time, an intruder can find the original files.

- The solution is to use a program, such as Eraser, that really erases data. Such programs overwrite your sensitive data with gibberish, in effect, randomizing the information so that it can't be re-created.

You can set the program to delete the contents of your recycle bin once a day, once a week, or once a month.

Sharing Information Carefully

- As we said earlier, pay attention to your own behavior. Don't go to dodgy websites, don't post too much personal information on the web, and be careful what you say and do in public cyberspace—because it all gets recorded somewhere.

- Another way to stay safe on the Internet is to be careful about how you visit websites. There are two ways to access websites that are in common use today.
  - One is HTTP, which stands for "hypertext transfer protocol." The other is HTTPS, in which the S stands for "secure." If you browse to a website using HTTPS, then your system automatically encrypts any transmissions.

  - Not all websites can accept HTTPS, but you can use a program called HTTPS Everywhere that will use the secure system when possible.

- Often, when you visit a website, the site leaves behind information on your computer (a "cookie") to make your next visit go more quickly and easily. You can eliminate this information by running a program called Cookie Cleaner once a month or so.

- You can also browse the web without your history being stored using a free program called Tor. This program encrypts messages and Internet traffic so that your request to visit, say, www.whitehouse.gov is encrypted before it is passed along on the web. In addition, Tor builds a volunteer network of servers around the globe to "bounce" encrypted traffic in a way that evades detection.

- Take care in how you use and manage wireless connections at home and in public. At home, encrypt your wireless connections. (Look on the Internet for instructions to protect your particular brand of

wireless router.) Put your router in the basement rather than in the attic to make it more difficult to intercept your signal.

- Don't engage in confidential cyber activity on unencrypted connections, such as those at a coffee house or the airport. Nearby network users on laptops and cell phones can use readily available programs to intercept unencrypted wireless communications. Save all of your banking and online bill paying for your encrypted home network.

Don't use unencrypted connections, such as the free Wi-Fi offered at the coffee shop, to do your online bill paying or banking.

- Turn off the automatic login function of the Wi-Fi antenna on your computer, as well as on your iPhone, Android, and iPad. The only networks you should tell your devices to "remember" are the personal ones you trust—and give them unusual names, not common ones, such as "ATT" or "Linksys."

- Will these steps make you invulnerable? Absolutely not. Does this protection come without cost? Again, no; it costs money, time, and effort to implement effective personal security protocols. But in the end, underinvesting in cybersecurity is also fundamentally unwise. The steps we've talked about in this lecture aren't perfect, but they will make you a less attractive target, and that's worth the effort and cost.

Important Terms

intrusion detection system: A computer security system that detects and reports when intrusions have occurred and a firewall has been breached.

Suggested Reading

Mitnick, *The Art of Deception*.

National Cyber Security Alliance, *StaySafeOnline* (www.staysafeonline.org).

Rosenzweig, *Cyber Warfare*.

The Tor Project, Inc. (www.torproject.org).

Questions to Consider

1. Is all the work necessary to be safe online worth the effort?
2. What sorts of sensitive data will you put in your new encrypted file?
3. Have you ever done online banking at the coffee shop? Will you continue to do that?
4. Is your wireless router password protected?

Critical Infrastructure and Resiliency

Lecture 17

In the last lecture, we talked about ways to protect your own computer and activities on the web, but we need to look at the same issues for our larger infrastructure systems. Are there things the owners of infrastructure facilities and systems should be doing but aren't? As it turns out, there probably are. In this lecture, we'll also look at another way of thinking about cybersecurity—one that is generally not in vogue. We will ask whether or not we should stop planning for perfect security and, instead, think more in terms of resiliency and recovery. As you'll see, there may be good reason to adopt a course of action that plans for a little bit of failure.

Infrastructure Vulnerabilities

- As we've spoken about at some length, the vulnerabilities of American infrastructure are quite real. Perhaps even more troubling, they are growing every day. We are pushing our dependency on cyberspace forward faster than ever before, and the hole we are digging for ourselves is getting deeper.

- A recent example comes from the state of Washington, where the electric utility has reversed the idea of the smart grid to accommodate excess electricity generated by wind turbines during a storm.
  - The utility offloads excess power into the hands of volunteer customers. It might, for example, raise the temperature in a customer's water heater. Then, once the storm has passed, the customers can return the stored energy to the grid.

  - Such energy storage systems are turned on and off through remote communications enabled by cyberspace technology, which means that they're vulnerable. Whenever any control system is linked to the Internet to give operators remote access, then it is also open to malicious actors who might want to hack the system.

- On a large scale, this might be a way to attack the power generation system. On a smaller scale, a hacker might be able to cause a heater in a single house to blow up as part of an assassination attempt.

- The utility system in Washington, like all utility systems, is operated by a SCADA system, and as we saw in Lecture 1, such systems are vulnerable. Remember, too, that SCADA systems run virtually every utility and manufacturing plant around the globe. We can imagine any number of worst-case scenarios, ranging from blackouts to floods to even a nuclear meltdown at the hands of cyber hackers.

Accepting Reality

- Our approach to protecting cyber systems today seems to be limited to hunkering down in defense, behind firewalls, antivirus programs, and intrusion protection systems. But another way to approach private-sector cybersecurity might be to become resigned—in a good way—to reality, to the fact that "stuff happens."

- The reality of failure is a truism of the world, and it's a particular truism for the cyber domain. For better or worse, cyber breaches are inevitable. A cybersecurity strategy that is premised on the possibility of a perfect defense and 100 percent protection against attacks is a practical impossibility. If that's the case, perhaps our planning should be based on the assumption that at least some attacks will succeed.

- Many systems incorporate expectations of possible failure, any one of which would serve as a good model. The electric grid itself, in fact, is not designed to work 100 percent of the time. Everyone knows that blackouts can occur, and the principal goal of the electric grid management system is to make sure that power is rapidly restored. The system anticipates and plans for some level of failure. Cybersecurity policy could do the same.

- One intriguing way to think about cybersecurity is to use our medical and public health-care system as a mental model. In many ways, cybersecurity maps very well onto the basic structure of diagnosis and treatment. Just as we never expect everyone to remain perfectly healthy, we should never expect every computer system to remain free of malware.
    - As in the medical system, our first set of cyber rules would deal with disease or infection prevention. In the health-care world, these are often simple steps related to personal hygiene, such as washing your hands. Similarly, in the cyber domain, good cyber hygiene, such as using strong passwords, is a good candidate for success in limiting the number of infections. Much of the public policy that would advance these goals involves simple education.

    - The next part of the analogy is vaccination. Almost every American has gotten required vaccinations before going to school, and we can easily imagine using the same concept in relation to antivirus programs. Just like vaccination in the physical world, cyber vaccine requirements could cut down on some of the more common virus infections.

    - When a disease outbreak occurs, our health-care system floods resources to the site of the infection to combat it and quarantines those who have been exposed to the disease so that they can't spread it. The cybersecurity model can also map onto this structure. When a company finds malware on its systems, it typically floods resolution resources to the infected portions of the system and takes the compromised server offline—quarantines it—until it is fixed.

    - Still other aspects of our public health system might have echoes in the cyber domain. Just as the Centers for Disease Control and Prevention (CDC) tracks the outbreaks of various diseases, we need to think of the **U.S. Computer Emergency Readiness Team (US-CERT)** as the cyber equivalent of the

CDC. This might require us to expand US-CERT and give it greater authority to collect information on cyber viruses.

- We also need excess hospital bed capacity to deal with epidemic infections, and we need something similar—excess bandwidth capacity—in the cyber domain to deal with denial-of-service outbreaks.

- Perhaps most important, the conceptualization of cybersecurity as an analog to public health brings with it a fundamental change in our thinking. It would help us recognize that an effort to prevent all cyber intrusions is as unlikely to succeed as an effort to prevent all disease. The goal is to prevent those infections that are preventable, cure those that are curable, and realize that when the inevitable illness happens, the cyber system, like the public health system, must be designed to continue operating.

Resiliency

- Though the analogy is not perfect, the medical model starts us thinking about one of the most significant questions we can ask in the cyber context: What does it mean to be resilient? In the cyber domain, resiliency means that our systems are robust, adaptable, and capable of rapid response and recovery. As noted by Franklin Kramer, a national security expert, to create systemwide resiliency, we need to use a mixture of techniques and mechanisms.

- The first building block for creating resiliency is diversity. We tend to think that genetic diversity is good for enabling the survival and adaptability of species, and the same is true for cyber systems. One way to foster resiliency is to build cyber systems with multiple forms of programming in their architecture. That way, any single form of attack is not successful against all systems.

- Another important building block of resiliency is redundancy. This means frequently creating snapshots of critical systems at a time

and place where they are working in a known and stable condition to enable restoration, if necessary.

- We can also increase resiliency by how we actually build systems. Today, infrastructure providers link all of their activities together in a series of servers. We can do much better by isolating and segregating different parts of a cyber system from one another. That way, any infected parts can be isolated so that a single failure will not cascade across the entire system.

- A corollary here is the idea that we need to watch what is happening inside cyber systems, not just guard the entry points. Advanced persistent threats can be resident, unobserved within a cyber system for long periods of time. Internal monitoring is necessary to give a better sense of when and how intrusions occur. In fact, one of the most important things a company can do to catch intrusions is to watch what traffic is leaving its system—that's where the real evidence of intrusion will be found.

© Ryan McVay/Photodisc/Thinkstock.

Better personnel screening and limited-access privileges are additional precautions companies can take against malicious intrusion.

- If, as we have discussed, cybersecurity is often a human problem, then infrastructure operators also need to think hard about who gets access to which portions of their systems. Many intrusions are made by insiders who take advantage of their access to install malicious software. In addition to better personnel screening , another effective precaution is to ensure that the people who are given access to a system get the least amount of privileged access necessary to achieve their purposes.

- A final component of resiliency is, surprisingly, to foster change. If targets of attack are concentrated in a single place and protected by an unchanging defense, a malicious intruder has a fixed objective against which to direct resources. If an infrastructure provider distributes targets widely and varies the defense, its system will be better able to frustrate an attack.

Deterrence

- As you'll recall, a "hack back" involves, in its most simple form, hacking into an attacker's computer to defeat his or her attempts to hack you. There are actually many flavors of hack backs, including measures that cause damage to a would-be attacker, measures that ensnare hackers with honeypot traps, preemptive attacks on parties who have shown some intent to hack, and more.

- As we saw in our lecture on cyber crime, most active defenses are almost certainly crimes under U.S. law. After all, a defensive attack will usually involve accessing a computer without the authorization of its owner. Thus, almost every aspect of private-sector self-help is, in theory, a violation of the Computer Fraud and Abuse Act. There are even more stringent limits on hack backs if the attacker is the representative of a nation-state.

- What should a company do if an imminent attack against its infrastructure is coming from a state-sponsored attacker? Will its efforts to defend itself violate the law? Despite the legal uncertainties, new companies are springing up with the sole purpose of providing offensive response options for companies under attack.

- The graphic representation of malware attacks at map.honeynet.org gives you an idea of the breadth of our vulnerability. For some, this suggests that playing only firewall defense is a losing strategy. We need to systematically go on the offense and plan for failure. Both strategies are the powerful realities of the cyber domain today.

Important Term

United States Computer Emergency Readiness Team (US-CERT): A component of the Department of Homeland Security. Its mission is to serve as a central clearinghouse for information concerning cyber threats, vulnerabilities, and attacks, collecting information from government and private-sector sources and then widely disseminating that information to all concerned actors.

Suggested Reading

Charney, *Collective Defense*.

Karas, Moore, and Parrot, *Metaphors for Cybersecurity*.

Rosenzweig, *Cyber Warfare*.

Questions to Consider

1. What are some of the downsides of the hack back? Will it lead to vigilantism, for example? If we don't permit hack back, does that mean that we must require the government to do all the protection for us?

2. Do you think the medical model is too pessimistic? After all, it starts from the idea that we're going to fail. Shouldn't we plan to succeed?

3. Think of all the things that are in your house or car that are connected to the network. What's the worst thing that could happen to you if someone targeted you personally through those systems?

Looking Forward—What Does the Future Hold?

Lecture 18

Hardly a day passes in America without a media story about cybersecurity. In just the last few years, President Obama crafted a new cyberspace policy and appointed a "cyber czar," competing cyber bills clamored for attention in the Senate, the Department of Defense announced a new Cyber 3.0 strategy, and more. Yet risks still abound. In the end, the cybersecurity policy that the United States adopts will determine how billions of dollars in federal funding are spent and have immeasurable consequences on privately owned critical infrastructure in America and on individual lives. In this final lecture, we will take a look forward to see what the future may hold for cyberspace and cybersecurity.

Some Basic Observations on Cyberspace

- Cyberspace is everywhere. The Department of Homeland Security has identified 18 sectors of the economy, covering everything from transportation to the defense industrial base, as the nation's critical infrastructure and key resources. Virtually all of those sectors now substantially depend on cyber systems, which are subject to real and powerful dangers.

- The fundamental characteristic of the Internet that makes it truly different from the physical world is that it lacks any boundaries. It spans the globe, and it does so nearly instantaneously. There is no kinetic analog for this phenomenon; even the most globe-spanning weapons, such as missiles, take 33 minutes to reach distant targets.

- As we discussed, the Westphalian age of cyberspace looms. One of the critical questions that lies ahead of us is the nature of Internet governance. Today, for the most part, rules about the Internet domain are set by nonprofit international organizations, but that state of affairs is being challenged. Sovereign nations seek to exert control, putting their own interests ahead of any international interest in an open Internet community.

- The fundamental anonymity of the Internet is nearly impossible to change. As originally conceived, the cyber domain serves simply as a giant switching system, routing data around the globe. It embeds no other function (such as verification of identity or delivery) into its protocols. Regardless of whether this anonymity is good or bad, it is here to stay. Yet paradoxically, for innocent Internet travelers, the veil of anonymity can be readily pierced.

- Cybersecurity is in the midst of its Maginot Line period, but such defenses never work in the long run. Instead of merely standing guard at Internet system gateways, we need to look beyond those gateways to assess patterns and anomalies. With that sort of information, cybersecurity could transition from detecting intrusions after they occur to preventing intrusions before they occur.

- It is a certainty that our protective cyber systems will be ineffective. No matter how well constructed, the cyber domain is sufficiently asymmetric that defeat is inevitable. Someday, somewhere, a cyber attack or intrusion will succeed in ways that we can hardly imagine, with consequences that we cannot fully predict. It follows that a critical component of any strategy is to plan for inevitable failure and recovery.

- Finally, we must be aware that the cyber domain is a dynamic environment that changes constantly. Today, people use the Internet in ways they didn't imagine just a few years ago. Anything the United States or the international community does in terms of legislation or regulation must emphasize flexibility and discretion over mandates and proscriptions.

Cloud Computing

- Cloud computing is the new, developing "in thing." Soon, its use will become widespread. The "cloud" is a name for a variety of services to which consumers are connected through the Internet. Cloud systems allow for significant economies of scale. Using them is often both cheaper and more efficient.

The use of cloud computing is rapidly becoming widespread; indeed, the federal cloud computing strategy is called "Cloud First."

- "On-demand software" is being developed that allows users to access the program and its associated data directly from the cloud. Users don't need to have the data or programs on their own laptops or systems; all they need are programs that let them pull down what they want from the cloud. We sometimes call these less-capable systems "thin clients."

- We can think of the cloud as a platform, an infrastructure, or a service, but all these conceptions share a common theme: The user does not manage or control the underlying cloud infrastructure of servers, operating systems, or storage hubs. Instead, the user has access to the data or applications on an as-needed basis from the cloud service provider.

- The cloud will bring with it some real potential security benefits. When malware attempts to execute in the cloud context, it does so on software that is only virtually connected to your hardware device. This often limits or modifies the malware's capacity for

harm. Cyber attacks may be significantly harder to accomplish in a cloud-oriented system.

- In addition, the cloud permits the creation of systems with different trust levels at different tiers of interaction. Low-level users get only a limited set of permissions and access. The capacity for malfeasance is limited by the inherent structure of the system, and the only people who can actually corrupt the system are the cloud providers.

- However, the tiered structure creates a greater potential for a catastrophically successful attack. Security works at the client level in cloud systems precisely because the cloud system owner is, in effect, "god." The owner controls all the resources and data at the cloud provider level. That means that a successful attack at this god level will have even worse consequences; low-level users may not even know that the system has been compromised.

- Of equal concern is the challenge of identifying a trustworthy god. Cloud computing may make human corruption concerns less frequent, but the effects of a security compromise may be much greater. Whom would we trust to be the "electrical grid god," for example?

- Another consequence of cloud computing is a return to the 1980s in terms of how computer systems operate; that is, the thin client is equivalent to the "dumb" terminal, and the cloud is equivalent to the mainframe. That centralized system of control is fundamentally authoritarian. The individual user in the cloud loses much of the independence that has made the web a fountain of innovation and invention.

Virtual Worlds

- Virtual worlds are a bit like Internet chat rooms. Users create online personas called "avatars" that interact with other avatars in a created space that mimics physical reality. Like cloud computing, this unusual phenomenon comes with both promise and peril.

- Virtual worlds today include sophisticated games, such as World of Warcraft, and systems that realistically mimic the real world, complete with economic and social interactions, such as Second Life. These worlds exist on the Internet but are distinct from traditional cyber systems and, in many ways, defy our ability to monitor actions that occur in them.

- Given the degree to which virtual worlds seek to simulate the real world, we should not be surprised that we face all the same sorts of potential for criminal or other malevolent behavior in these environments that we find in real life. Already, we have seen sophisticated securities frauds that have virtual-world consequences.

- Different risks arise from other interactions between the virtual world and real-world events. National security may be threatened, for example, when digital currencies are traded in a virtual world in a manner that results in the real-world transfer of funds for the purposes of money-laundering. The trading of real and virtual funds is, in effect, an unregulated system of exchange. Because the core of most virtual worlds is a functioning "economy," the system is ripe for manipulation.

Gated Internet Communities

- As we've discussed, the Internet was built without authentication as a protocol; thus, any security functionality is, by definition, an "add-on" function. Why not start over again with a structure that has greater built-in security provisions? Although it is nearly impossible to imagine that the existing cyber domain will ever disappear, it is quite plausible to imagine that a series of alternate Internets might be created.

- This is particularly likely to be tried by those whose primary concerns are for security rather than freedom or privacy. For example, U.S. Cyber Command head General Keith Alexander has already floated the concept of a ".secure" network for critical services, such as banking, that would be walled off from the public

Internet. Access to .secure could be limited to those who submitted to an identity check.

- In the end, however, one suspects that the trend to walled gardens will be limited. They may well become prominent in authoritarian countries, but within the more liberal Western democracies, their utility will likely be limited to certain specialized areas, such as military and financial networks.

Quantum Computing

- The entire structure of the Internet (and, thus, all of its power and danger) is tied to the technology that undergirds it: the integrated silicon chip. That chip, at the heart of every computer, is the physical mechanism that creates the 1s and 0s of binary code and drives the Internet. What if chips were no longer the basis for Internet computing?

- We may be standing on the threshold of such a change. Physicists have developed the concept of a quantum computer, that is, a computer whose operations are based on theories of quantum physics in the same way that our current crop of computers is based on the operation of classical Newtonian physics.

- If ever created, quantum computers would make the power of contemporary computers look puny by comparison. They would be smaller, faster, and possibly cheaper in the long run, meaning that we might see a day when your computer is a small appliance you wear as a pinky ring.

- As we know, however, vast computing power brings with it some obvious dangers. For example, current encryption programs based on large prime-number multiplication are amazingly robust and difficult to break. But theoretical physicists have shown that, for a quantum computer, the breaking of prime-number encryption codes would be trivial.

Summing Up the Future

- In some ways, the future is a bit unsettling. If you think the Internet and cyberspace are confusing and cutting edge today, imagine what they might be like tomorrow.

- On the other hand, perhaps it's not so unsettling after all. If you've learned anything in this course, it should be that cyberspace is remarkable and useful precisely because it is open and unstructured. That openness brings risks and dangers that cannot be eliminated, but they can often be understood, managed, and reduced.

- We will always face the same problem: how to reap all the benefits to be gained from increases in efficiency and productivity while minimizing the risks of harm. The challenge of achieving that goal is one of the things that makes this area of technology, law, and policy so interesting and exciting.

Suggested Reading

Gardner, *Future Babble.*

Hawkins, *On Intelligence*.

Rosenzweig, *Cyber Warfare*.

Taleb, *Black Swan*.

Questions to Consider

1. Think of how your use of cyberspace has changed in the last 20 years, or 10, or 5. Do you think you will see more change in the next 20 years or less?

2. What's the most unusual thing you can possibly imagine happening in cyberspace?

3. Isn't "do no harm" a prescription for cowards? Shouldn't we dare to seek and embrace change in the dynamic world of cyberspace?

Glossary

Anonymous: A loose collective group of cyber hackers who espouse Internet freedom and often attack websites that they consider symbols of authority.

botnet: A network of computers controlled by an outside actor who can give those computers orders to act in a coordinated manner, much like orders to a group of robots.

Comprehensive National Cybersecurity Initiative (CNCI): The broad federal strategy for fostering cybersecurity in America. When first drafted in 2008, it was classified. An unclassified version was publicly released in 2010.

Cyberspace Policy Review: In May 2009, one of the first actions of the Obama administration was the development and release of a broad-based cyberspace policy review. This review has guided federal strategy since then.

denial-of-service attack: An attack in which a malicious actor repeatedly sends thousands of connection requests to a website every second. The many malicious requests drown out the legitimate connection requests and prevent users from accessing the site.

distributed denial of service (DDoS): A DDoS attack is related to a denial-of-service attack, but in a DDoS attack, the attacker uses more than one computer (often hundreds of distributed slave computers in a botnet) to conduct the attack.

domain name system (DNS): The DNS is the naming convention system that identifies the names of various servers and websites on the Internet. In any web address, it is the portion of the address after http://www. One example would be microsoft.com.

domain name system security extension (DNSSEC): A proposed suite of security add-on functionalities that would become part of the accepted

Internet protocol. New security features will allow a user to confirm the origin authentication of DNS data, authenticate the denial or existence of a domain name, and ensure the data integrity of the DNS.

Einstein: Intrusion detection and prevention systems operated by the federal government, principally to protect federal networks against malicious intrusions of malware.

encryption: The act of concealing information by transforming it into a coded message.

firewalls: Computer security systems designed to prevent intrusions.

hacktivist: A combination of the words "hacker" and "activist." The term denotes a hacker who purports to have a political or philosophical agenda and is not motivated by criminality.

Information Sharing and Analysis Center (ISAC): A cooperative institution chartered by the federal government that brings together sector-specific private-sector actors to share threat and vulnerability information. There are ISACs for the financial sector, the chemical industry, the IT sector, and most other major private-sector groups.

Internet Corporation for Assigning Names and Numbers (ICANN): A nonprofit organization that sets the rules for creating and distributing domain names. Originally chartered by the U.S. government, it now operates on a multilateral basis from its headquarters in California.

Internet Criminal Complaint Center (IC3): The IC3 is a unit of the U.S. Department of Justice. It serves as a central collection point for complaints of criminal cyber activity and provides estimates of criminal effects.

Internet Engineering Task Force (IETF): A self-organized group of engineers who consider technical specifications for the Internet. The IETF sets voluntary standards for Internet engineering and identifies "best current practices." Though the organization has no enforcement mechanism, IETF standards are the default for all technical Internet requirements.

Internet protocol (IP) address: An IP address is the numeric address that identifies a website on the cyber network. Typically, it looks like this: 172.16.254.1. Using the IP address, information can be communicated from one server to another. One of the critical functions of the DNS is to translate domain names (which appear in English) into numerical IP addresses.

Internet Systems Consortium (ISC): A nonprofit 501(c)(3) corporation that produces open-source software to support the infrastructure of the Internet. Its work is intended to develop and maintain core production-quality software, protocols, and operations.

intrusion detection system: A computer security system that detects and reports when intrusions have occurred and a firewall has been breached.

keylogger: As the name implies, a keylogger program is one that records all the keystrokes entered on a keyboard (such as the letters and numbers in a password) and then reports those keystrokes to whoever installed the program.

letters rogatory: Formal letters of request for legal assistance from the government of one country to the courts of a foreign country. This is the mechanism by which mutual legal assistance treaties are implemented.

logic bomb: A program that tells a computer to execute a certain set of instructions at a particular signal (a date or a command from outside, for example). Like many bombs or mines, the logic bomb can remain unexploded and buried for quite some time.

malware: Short for "malicious software." A general term describing any software program intended to do harm.

microblogs: Systems, such as Twitter, that allow blogging on the Internet but only on a "micro" scale. Twitter, for example, is limited to 140 characters per post.

mutual legal assistance treaty (MLAT): An agreement between nations to exchange information in support of investigations of violations of criminal or public law.

National Counterintelligence Executive (NCIX): Part of the Office of the Director of National Intelligence. The mission of the NCIX is the defensive flip side of our own espionage efforts. It is charged with attempting to prevent successful espionage against the United States by our adversaries.

peer-to-peer: Most Internet transmissions involve some routing by intermediate servers that serve a controlling function. Peer-to-peer systems, as the name implies, enable direct communications between two (or more) endpoints without the need for intermediate routing and with no centralized or privileged intermediary.

phishing: Phishing is a cyber tactic that involves dangling "bait" in front of an unsuspecting user of the Internet. The bait may be an e-mail with an attractive link to click on that takes the unwary user to a malicious site.

SCADA (supervisory control and data acquisition): SCADA systems are used to control industrial processes, such as automobile manufacturing. They can be, but are not necessarily, controlled by other computer operating systems.

spear-phishing: A phishing attack that is targeted at a particular, specific recipient; the name comes from the similarity of using a spear to catch a particular fish.

Trojan horse: As the name implies, a computer program or message that, on the outside, looks like an innocent piece of code. Contained within the code, however, is a malicious piece of software.

United States Computer Emergency Readiness Team (US-CERT): A component of the Department of Homeland Security. Its mission is to serve as a central clearinghouse for information concerning cyber threats, vulnerabilities, and attacks, collecting information from government and

private-sector sources and then widely disseminating that information to all concerned actors.

virus: A piece of computer code that infects a program, much as a virus infects a person, and replicates itself.

WikiLeaks: A website founded by Julian Assange. It accepts anonymous leaks of classified, secret, and confidential information and then posts the information in an effort to promote transparency. Controversial in operation, WikiLeaks' most famous leak was of more than 250,000 classified State Department cables.

wiretapping: The interception of a message in transit by someone who is not the intended recipient. The term comes from the practice of attaching two clips to a copper telephone wire to intercept a phone call.

worm: A stand-alone program that replicates itself. It often hides by burrowing in and concealing itself amidst other program code, like a worm in dirt.

zero-day exploit: A vulnerability in a software program that has not previously been used or discovered. Because most vulnerabilities are quickly patched after they become known, zero-day exploits, which are not yet patched, are valuable to malicious actors. They leave systems open to intrusions that will be successful on the "zeroth" day.

Bibliography

Computers and the Internet—General Information

Gleick, James. *The Information: A History, a Theory, a Flood.* New York: Pantheon, 2011.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press, 2006.

Lessig, Lawrence. *Code Version 2.0.* New York: Basic Books, 2006.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom.* Ann Arbor, MI: Public Affairs, 2011.

Post, David G. *In Search of Jefferson's Moose: Notes on the State of Cyberspace.* Oxford: Oxford University Press, 2009.

Reid, T. R. *How Two Americans Invented the Microchip and Launched a Revolution.* New York: Random House, 2001.

Zittrain, Jonathan. *The Future of the Internet and How to Stop It.* New Haven: Yale University Press, 2008.

Counterterrorism

Baer, Martha, Katrina Heron, Oliver Morton, and Evan Ratliff. *Safe: The Race to Protect Ourselves in a Newly Dangerous World.* New York: HarperCollins, 2005.

Baker, Stewart. *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism.* Washington, DC: Hoover Institution, 2010.

Chesney, Robert. "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate." *Journal of National Security Law & Policy* 5 (2012): 539.

George, Roger Z., and Harvey Rishikof, eds. *The National Security Enterprise: Navigating the Labyrinth.* Washington, DC: Georgetown University Press, 2011.

Schmitt, Eric, and Thom Shanker. *Counterstrike: The Untold Story of America's Secret Campaign against Al-Qaeda.* New York: Macmillan, 2011.

Cybersecurity—General Information

Charney, Scott. *Collective Defense: Applying Public Health Models to the Internet.* Redmond, WA: Microsoft Corporation, 2010.

"Cybersecurity Symposium." *Journal of National Security Law & Policy* 4, no. 1 (2010).

Executive Office of the President. *National Strategy for Trusted Identities in Cyberspace.* April 2011.

Karas, Thomas, Judy Moore, and Lori Parrot. *Metaphors for Cybersecurity.* Sandia National Laboratory, 2008.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara: Praeger, 2012.

———. www.cyberwarfarebook.com.

U.S. Department of Justice, Office of Legal Counsel. "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch." August 2009.

———. "Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch." January 2009.

Data Mining and Government Databases
Bailey, Dennis. *The Open Society Paradox: Why the 21st Century Calls for More Openness—Not Less.* London: Brassey's, 2004.

Harris, Shane. *The Watchers: The Rise of America's Surveillance State.* New York: Penguin Press, 2010.

Markle Foundation. *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force.* 2002.

———. *Creating a Trusted Network for Homeland Security.* 2003.

O'Harrow, Robert, Jr. *No Place to Hide.* New York: Free Press, 2005.

Smith, Derek V. *Risk Revolution: The Threats Facing America and Technology's Promise for a Safer Tomorrow.* Athens, GA: Longstreet Press, 2004.

Economics
Fisher, Eric A. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions.* Hauppauge, NY: Nova Science Publishers, 2009.

Grady, Mark F., and Francesco Paris, eds. *The Law and Economics of Cybersecurity.* Cambridge: Cambridge University Press, 2006.

Ostrom, Elinor. *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge: Cambridge University Press, 1990.

Powell, Benjamin. "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry." *Journal of Law, Economics & Policy* 1 (2005): 497.

Thaler, Richard, and Cass Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness.* New Haven: Yale University Press, 2008.

Encryption and Wiretapping
Al-Kadi, Ibraham A. "The Origins of Cryptology: The Arab Contributions." *Cryptologia* 16, no. 2 (April 1992).

Gardner, Martin. "A New Kind of Cipher That Would Take Millions of Years to Break." *Scientific American* 237 (August 1977).

Landau, Susan. *Surveillance or Security: The Risks Posed by New Wiretapping Technologies.* Cambridge, MA: MIT Press, 2011.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age.* New York: Penguin Press, 2001.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

Espionage and Crime
Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare.* New York: Penguin Press, 2011.

Office of the National Counterintelligence Executive. *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.* October 2011.

U.S.-China Economic and Security Review Commission. *Report to Congress.* November 2010.

VeriSign. *The Russian Business Network: Rise and Fall of a Criminal ISP.* March 2008.

The Future
Gardner, Dan. *Future Babble: Why Expert Predictions Are Next to Worthless, and You Can Do Better.* New York: Dutton, 2011.

Hawkins, Jeff. *On Intelligence: How a New Understanding of the Brain Will Lead to the Creation of Truly Intelligent Machines.* New York: Henry Holt, 2004.

Taleb, Nassim. *Black Swan: The Impact of the Highly Improbable.* New York: Random House, 2007.

Government Organization

Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency.* December 2008.

Executive Office of the President. *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* May 29, 2009.

———. *Comprehensive National Cybersecurity Initiative.* 2010 (declassified version).

U.S. Department of Homeland Security and National Security Agency. *Memorandum of Understanding Regarding Cybersecurity.* October 10, 2010.

Hardware Problems

Defense Science Board. *Mission Impact of Foreign Influence on DoD Software.* September 2007.

U.S. Department of Commerce. *Defense Industrial Base Assessment: Counterfeit Electronics.* January 2010.

International Cybersecurity

Demchak, Chris, and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring 2011).

Executive Office of the President. *International Strategy for Cyberspace.* May 2011.

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." In *Future Challenges in National Security and Law*, edited by Peter Berkowitz. Washington, DC: Hoover Institution, 2011.

Malware
Alperovitch, Dmitri. *Revealed: Operation Shady RAT.* McAfee, August 2011.

Bowden, Mark. *Worm: The First Digital World War.* New York: Atlantic Monthly Press, 2011.

Combating Robot Networks and Their Controllers: A Study for the Public Security and Technical Program (unclassified version 2.0). May 6, 2010.

Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network." March 2009.

Symantec, W32.Stuxnet Dossier. February 2011.

Personal Cybersecurity
Mitnick, Kevin. *The Art of Deception: Controlling the Human Element*. Hoboken, NJ: Wiley, 2002.

National Cyber Security Alliance. *StaySafeOnline*. www.staysafeonline.org.

The Tor Project. www.torproject.org.

Privacy and Secrecy
American Bar Association, Office of the National Counterintelligence Executive, and National Strategy Forum. *No More Secrets: National Security Strategies for a Transparent World.* March 2011.

Mayer-Schoenberger, Victor. *Delete: The Virtue of Forgetting in the Digital Age.* Princeton, NJ: Princeton University Press, 2009.

Raul, Alan Charles. *Privacy and the Digital State: Balancing Public Information and Personal Privacy.* New York: Kluwer Academic Publishers, 2002.

Rosen, Jeffrey. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age.* New York: Random House, 2004.

Solove, Daniel J., and Paul M. Schwartz. *Privacy, Information and Technology.* 2nd ed. Alphen aan den Rijn, Netherlands: Wolters Kluwer, 2009.

Warfare

Carr, Jeffrey. *Inside Cyber Warfare.* Cambridge, MA: O'Reilly, 2010.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins, 2010.

Kramer, Franklin, Stuart Starr, and Larry Wentz, eds. *Cyberpower and National Security.* Washington, DC: National Defense University, 2009.

Libicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND, 2009.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 97 (September/October 2010).

Nye, Joseph S., Jr. *Cyber Power.* Cambridge, MA: Harvard Belfer Center, 2010.

———. *Soft Power: The Means to Success in World Politics.* Ann Arbor, MI: Public Affairs, 2004.

Owens, William, Kenneth Dam, and Herbert Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*. Washington, DC: National Academies Press, 2009.

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: National Academies Press, 2010.

Rattray, George J. *Strategic Warfare in Cyberspace.* Cambridge, MA: MIT Press, 2001.

U.S. Department of Defense. *Strategy for Operating in Cyberspace.* July 2011.

———. *Cyberspace Policy Report.* November 2011.

U.S. Government Accountability Office. *Defense Department Cyber Efforts.* May 2011.