Introduction

Part I: How It All Works

1. cyberspace is the realm of computer networks in which information is stored, shared, and communicated online.
2. But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications.

Short History of The Internet

1. The brilliance of the model is how it breaks the communication into "layers" and allows each layer to function independently. These packets, in turn, can be sent over any type of network, from sound waves to radio waves to light pulses on a glass fi ber. Such Transport Control Protocols, or TCPs, could be used over all sorts of packet protocols, but we now use a type called the Internet Protocol, or IP, almost exclusively in the modern Internet.
2. In 1990, a researcher at the European research center CERN in Switzerland took a relatively obscure form of presenting information in a set of linked computer documents and built a new networking interface for it. With this HyperText Transfer Protocol (HTTP), and an accompanying system to identify the linked documents (URLs), Tim Berners-Lee "invented" the World Wide Web as we now look at it.
3. A few years later, researchers at the University of Illinois introduced the Mosaic web browser, which simplified both web design and introduced the new practice of "web surfing" for the general public.
4. The first thing your computer needs to know is how to find the servers that host the Brookings web page. To do that, it will use the Internet Protocol (IP) number that serves as the address for endpoints on the Internet. Your machine was most likely automatically assigned an IP address by your Internet service provider or whatever network you are using. It also knows the address of its router, or the path to the broader Internet. Finally, your computer knows the address of a Domain Name System server. The Domain Name System, or DNS, is the protocol and infra structure through which computers connect domain names (human memorable names like Brookings.edu) to their corresponding IP addresses (machine data like 192.245.194.172).
5. Entry into the club of top-level domains is controlled internationally through the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non profit organization created in 1998 to run the various Internet administration and operations tasks that had previously been performed by US government organizations.
6. Organizations, such as Brookings or Apple or the US Department of State, acquire their domains through intermediaries called registrars. These registrars coordinate with each other to ensure the domain names in each top-level domain remain unique.

7. Those networks, in turn, form nodes called Autonomous Systems (AS) in the global Internet. Autonomous Systems define the architecture of Internet connections.
8. Since there is no global address book, the nodes in the network have to share key information with other routers, like which IP addresses they are responsible for and what other networks they can talk to. This process happens separately from the Internet routing process on what is known as the "control plane."
9. understanding the Internet's basic decentralized architec ture provides two insights for cybersecurity
10. The IETF develops new Internet standards and protocols and modifi es existing ones for better performance.
11. While the IETF has no offi cial board or formal leadership, the Internet Engineering Steering Group (IESG) offers oversight and guidance for both the standards process and the standards them selves. In turn, the Internet Architecture Board (IAB), which evolved from the technical advisory board of the original ARPANET man agement in the early 1970s, offers further oversight of the IESG. Both of these organizations fall under the auspices of the Internet Society, or ISOC, an international group formed in 1992 that over sees most of the technical standards process
12. Identifi ers such as IP addresses and domains have to be unique—the Internet wouldn't work if multiple parties attempted to use the same IP address or wanted to resolve a domain name to a competing address.
13. The Internet Corporation for Assigned Names and Numbers, or ICANN, was born. While chartered in California as a nonprofi t, ICANN set in motion a structured way to distribute IP addresses that more appropriately refl ected the Internet's global nature
14. We reject: kings, presidents and voting. We believe in: rough consensus and running code.
15. Acquisti fi rst uses image-matching technology to fi nd your face on a social networking website. If your birthdate and birth city are listed online, as they are for most people, then he can use the patterns that link time and location to the fi rst fi ve of the nine numbers in your Social Security number. Then it is just a numbers guessing game for the remaining digits. If you come from a small state like Delaware, the Social Security number can be determined in less than 10 tries.
16. In the computer world, "identifi cation" is the act of mapping an entity to some information about that entity. Passwords can be guessed or broken and require a cognitive load (you have to memo rize them). If they are reused across different contexts, then breaking one system allows an attacker into others. Things that you "have" can be stolen or forged. And even biometrics can be compromised.
17. After authentication is authorization.Every activity on the Internet is data being routed from an Internet Protocol (IP) address. Instead, the IP address will be dynamic. The consumer's Internet service provider will assign an IP address for a period of time, but it might be reassigned to some

one else after the consumer disconnects. But it can provide some information about the geo graphic location and the means by which that individual accesses the Internet.

18. Relying on the IP address would be like relying on license plates to identify drivers. A sophisticated user can easily hide or dis guise her IP address by routing her activities through another point on the Internet, making it appear that that node was responsible for the original traffi c. Even the patterns of how individual users browse and click through a website can be used to identify them.
19. There's an old joke in the security industry about how to secure any computer: Just unplug it.

What Do We Mean by "Security" Anyway?

1. Security is associated with the presence of an adversary. In that way, it's a lot like war or sex; you need at least two sides to make it real.
2. three goals: Confi dentiality, Integrity, Availability, sometimes called the "CIA triad." Confi dentiality refers to keeping data private. Integrity means that the system and the data in it have not been improperly altered or changed without authorization. Availability means being able to use the system as anticipated.
3. Resilience is what allows a system to endure security threats instead of critically failing

What Are the Threats?

1. The Citigroup attack was about fi nancial fraud. The RSA attack was industrial theft, and Stuxnet was a new form of warfare.
2. In the attack on RSA, the attackers wanted key business secrets in order to spy on other companies. For Stuxnet (a case we'll explore further in Part II), the attackers wanted to disrupt industrial control processes involved in uranium enrich ment, so as to sabotage the Iranian nuclear program.
3. It is also important to consider whether the threat actor wants to attack you , or just wants to attack.
4. only three things you can do to a computer: steal its data, misuse credentials, and hijack resources.
5. Stolen data can reveal the strategic plans of a country or undermine the competitiveness of an entire industry. Stolen credentials can give the ability to change or destroy code and data, changing payrolls or opening up dams, as well as the ability to cover tracks. Hijacking resources can prevent a company from reaching customers or deny an army the ability to communicate.

One Phish, Two Phish, Red Phish, Cyber Phish: What Are Vulnerabilities?

1. stolen, over 300 in all, but that the cars were all of a particular brand, new BMWs.
2. First, they used radio frequency jammers to block the signal of a car's electronic key.
3. Once in the car, the thief would then plug into the OBD-II connector and then use that to obtain the car's unique key fob digital ID. Next, the thief would reprogram a blank electronic key to

correspond with the car's ID. Then they simply drove away, with the owner of the advanced luxury car none the wiser.

4. The case of the lost luxury cars is a good illustration of how build ing a complex system can create new openings and hidden vulner abilities that bad guys can try to exploit.
5. When the attacker has such "root access," the ability to execute any command, the victim is completely vulnerable, or what hackers call "pwned"
6. Fear is a powerful motivator. When a user's computer displays a message threatening to expose activities on a pornographic website, fear of exposure can motivate payment.
7. Phishing e-mails look like official e-mails from the vic tim's bank, employer, or some other trusted entity. They claim to require some action by the victim, perhaps to correct an account error or see a message on Facebook, and fool victims into visiting a web page where they are asked to enter their credentials.
8. "spear phishing." These target not just networks but key individuals inside those networks.
9. A good illustration is a SQL (pronounced "sequel") injection, one of the most common ways a website is attacked. Many web appli cations are built on Structured Query Language (SQL), a type of programming language used to manage data.
10. But an attacker, instead of enter ing a name and address as requested, can enter specifi cally crafted commands that the database will read and interpret as program code, rather than just data to be stored. These commands can be used to learn about the database, read data, and create new accounts. In some cases, access can be used to discover and change security set tings on the server, allowing the attacker to control the entire web system.
11. buffer overflow - If a program can be tricked into writing inputted data that is larger than expected, it can spill over the allocated "buffer," or storage area, and overwrite the space where the computer stores the next instruction to be executed. If that newly written memory space is then read and interpreted by the computer, the program can break or follow the attacker's instructions. - takes place at the system memory level.
12. Malicious software, or "malware," is a prepackaged exploitation of a vulnerability. There is often a "payload" of instructions detail ing what the system should do after it has been compromised. Some types of malware contain instructions for reproduction, in order to spread the attack. "Worms" spread themselves automatically over the network
13. Malware can also be spread over the Web via "drive-by" attacks, where the victim's only mistake is visiting the wrong website.
14. Botnet controllers can also leverage the network connec tions of their victims' systems to send spam, host websites to sell illegal products, or defraud online advertisers
15. DDoS attacks target the subsystems that handle connections to the Internet, such as web servers.
16. It's the equivalent of having thousands or even millions of people trying to call your phone.

17. Criminal gangs may go to a website and threaten to take it offl ine unless they pay for "protection."
18. During the initial stages of the crisis in Syria in 2011, supporters of the Syrian regime shared DDoS tools to attack critics of the government and news organizations that covered the grow ing violence.

How do we trust in cyberspace

1. Online trust is built on cryptography—the practice of secure communications that goes all the way back to the fi rst codes that Julius Caesar and his generals used to keep their enemies from understanding their secret messages.
2. A hash func tion takes any piece of data and maps it to a smaller, set-length output, with two specifi c properties.
3. "Asymmetric cryptography": The idea is to separate a secret key into a public key, which is shared with everyone, and a private key that remains secret. The two keys are generated such that something that is encrypted with a public key is decrypted with the corresponding private key, and vice versa
4. Asymmetric cryptography requires some means of trusting the public keys. In most modern systems we rely on a "trusted third party." These are organizations that produce signed digital "certifi cates" that explic itly tie an entity to a public key
5. When we visit HTTPS web addresses and get the little lock icon to verify the secure connection, we are visiting a secure website and are trusting the certifi cate authorities. Our web browsers ask the secure domain for its public key and a certifi cate signed by a CA, tying the public key explicitly to the Internet domain.
6. If someone can steal a CA's signing key, then the thief (or whoever they pass the key on to) could intercept "secure" traffi c without the victim noticing. It is hard to pull off, but it has been done. In 2011, someone (later leaks fi ngered the NSA) stole a Dutch CA's keys and used them to inter cept Iranian users' access to Google's Gmail.

What Is an Advanced Persistent Threat (APT)?

1. An APT starts with a specifi c target. The team knows what it wants and who it is going after to get it. APT targets have ranged from military jet designs to oil company trade secrets.
2. online search tools and social networking have been a godsend to the attackers.
3. Another effort, which American national security offi cials have blamed on Chinese intelligence and military units, gathered details not only on targets' key friends and associates but even what farewell they typically used to sign off their e-mails (e.g., "All the best" vs. "Best regards" vs. "Keep on Trucking") to mimic it for a spear phishing attack vector.
4. These attackers frequently use spear phishing and faked e-mails, with some exploit hidden inside triggering a download of malware.

5. Like other businesses, APT groups often conduct dry runs and even “quality assurance” tests to minimize the number of antivirus programs that can detect them.
6. Other APTs have, for example, used networks like Facebook to fi nd friends of individuals with a high level of privilege inside a targeted network. Then they compro mise these friends’ instant messaging chats to sneak in. Perhaps the most interesting example of this use of social networking tools saw senior British offi cers and defense offi cials tricked into accepting “friend requests” from a faked Facebook account that claimed to be Admiral James Stavridis, the commander of NATO. Who wouldn’t want an admiral as a friend; imagine their disappointment when it turned out to be a hacker!
7. Once the team is in, they branch out like a viral infection, often with more personnel joining the effort. They jump from the initial footholds, compromising additional machines inside the network that can run the malware and be used to enter and leave. This often involves installing keystroke-logging software that tracks what people are typing and a “command and control” program that can direct the malicious code to seek out sensitive information. At this point, the target is “pwned.”
8. French offi cials, for example, have accused APTs linked to Chinese intelligence of gaining access to the computers of several high-level French political and business lead ers and then activating microphones and web cameras so that they could eavesdrop on conversations. Even more nefarious are those that don’t simply steal data but also alter fi les, which as we explore later can have major consequences. This ultimately shifts the APT from an act of crime or espionage to an act of sabotage or even war. The exfi ltration phase, when massive amounts of data leave the network (such as when an entire e-mail fi le exits), is actually when many successful APTs are detected.
9. Exfiltration teams therefore use all sorts of tricks to sneak the information out and then hide their tracks. One common tactic involves routing data through way stations in multiple countries, akin to a money launderer running stolen funds through banks all over the world. This not only makes it more difficult to track them down, but also routes the APT’s activities through differ ent countries and legal jurisdictions, ultimately complicating prosecution.
10. Finding which machines inside the system have been infected can take months.
11. They will literally yank hard drives out of their com puters and post handwritten signs in the hallways about password policy changes.
12. Except in cases where the attackers are sloppy (our favorite example being when a high-ranking Chinese military offi cer employed the same server to communicate with his mistress and coordinate an APT)

How Do We Keep the Bad Guys Out?

1. McAfee “malware zoo” is what the computer security firm calls its collection of the various types of malicious or malevo lent software (known as “malware”) designed to wreak havoc on Internet users.
2. Traditional antivirus soft ware relies on detecting these “signatures.” The programs scan all files on the system as well as incoming traffic against a dic tionary of known malware, looking for anything that matches these signatures of malice.
3. The very same attack can be made into very different signatures, disguised by programs that automatically generate new features.
4. Modern antivirus don’t just screen, they use “heu ristic” detections to identify suspicious computer code behavior based on rules and logical analysis. Static analysis breaks apart the computer code and looks for patterns associated with the behavior of an attacker. Virtual machines and other sophisticated defenses dynamically simulate the code operation to determine whether the fi le examined will misbehave without putting the actual system at risk.
5. The simplest form of network defense is a “firewall.” computer firewalls are like filters that reject traffic based on specific rules. “Intrusion detection systems” exist at the com puter level or on the network. They detect attack signatures and identify anomalous behavior.
6. These systems alert administrators to potential attacks and keep logs for detailed forensic analysis. In cybersecurity terms, an air gap is a physical separation between the network and critical systems.
7. Similarly, maintaining an air gap is often unrealistic, as the Iranians discovered when their supposedly air-gapped systems still got infected by the Stuxnet virus. Best defense is a good offense.
8. But the only other option is to close the zoo and let the malware animals run free.

Who Is the Weakest Link? Human Factors

A particular hub that has drawn unwanted attention is the Second Bureau of the Third Army, Unit 61398, also known in cybersecurity circles as the “Comment Crew” or “Shanghai Group.” This is a key unit tasked with gathering political, economic, and military-related intelligence on the United States through cyber means.

Part II WHY IT MATTERS

What Is the Meaning of Cyberattack? The Importance of Terms and Frameworks

Whodunit? The Problem of Attribution

“patriotic hacker” communities and other nonstate groups, including student and even cybercriminal groups, have been mobilized by their governments for such purposes.

What Is Hactivism?

1. Recent sit-ins have targeted physical location, such as a specifi c government building, by trying to overwhelm the networks and devices at that site with large geotagged fi les, such as YouTube videos.

2. When an attack focuses on an individual's personal information, it's referred to as "doxing," as in revealing personal documents publicly.
3. They gained access to the company's networks, and through them, the fi rm's entire life cycle, including the names and home addresses of all its employees, shareholders, customers, and business partners. They published all these names and addresses online, even those of the fi rm's cater ers and cleaners. Many of these individuals and companies were subsequently targeted in a strategy to undermine "every critical relationship of a company necessary to thrive."

Focus: Who Is Anonymous?

The members then use various media such as Twitter, Facebook, and YouTube to distribute "attack posters" to announce the plans, further coordinate steps, and draw new volunteers from around the world into the attacks, building up the ranks of an "Anonymous" army of hactivists.

The Crimes of Tomorrow, Today: What Is Cybercrime?

1. The most pervasive type of cybercrime is "credential fraud," or the misuse of account details to defraud fi nancial and payment sys tems.
2. A common tool is the "phishing" e-mail, which poses as a communication from a fi nancial institution and presents a link where the victim is prompted to enter his credentials.
3. Criminals take advantage of advertising revenue by registering web domains just a few letters different from popular websites, or "typosquat ting," and collect ad revenue from the page visits by those with clumsy fi ngers. Enterprising scammers even take advantage of "trending" topics on the Web by quickly registering websites in the hopes of being seen by users searching for newly popular stories, again extracting advertising revenue. These attacks reduce the effi cacy of online advertising, which is the lifeblood of freely available content.
4. Their goal is to persuade the victim to deliver his or her money willingly. These efforts target our most basic human emotions: greed, fear, and love.

Shady RATs and Cyberspies: What Is Cyber Espionage?

"We should not forget that it was China where 'death by a thousand cuts' originated."

How Afraid Should We Be of Cyberterrorism?

1. Taking down hydroelectric generators or designing malware like Stuxnet that causes nuclear centrifuges to spin out of sequence doesn't just require the skills and means to get into a computer sys tem. It requires knowing what to do once you're there.
2. But the explosion of just one nuclear bomb, even a jury-rigged radiological "dirty bomb," would irradiate a city for centuries and set off an earthquake in global pol itics. Similarly, while a computer virus could wreak havoc in the economy, a biological weapon could change our very patterns of life forever.

So How Do Terrorists Actually Use the Web?

What about Cyber Counterterrorism?

1. metadata is information that describes the nature of communication, rather than the content.

2. It includes information about geographic location, time, e-mail addresses, and other technical details about the data being created or sent. When this data is gathered together from sources around the world, sophisticated algorithms can be used to connect dots and reveal new patterns, as well as track individual devices, even when the user is trying to hide her identity. The effort was designed to help fi nd links between terrorists.

Security Risk or Human Right? Foreign Policy and the Internet

Cloud computing, the concept of delivering computing resources remotely over a network, is both a multibillion-dollar industry and a growing fi eld that many believe is key to the future of the online world

Focus: What Is Tor and Why Does Peeling Back the Onion Matter?

1. A simple approach is a single-hop proxy, where you send your traffi c to a computer that then passes it along to the fi nal destination.
2. Tor is an "overlay network" that provides online protection against surveillance and traffi c analysis.

Who Are Patriotic Hackers?

"patriotic hacking," an action that involves citizens or groups within a state joining together to carry out cyberattacks on perceived enemies of that country.

Focus: What Was Stuxnet?

What Is the Hidden Lesson of Stuxnet? The Ethics of Cyberweapons "

"Unless you happen to be running a large array of exactly 984 Siemens centrifuges simultaneously, you have nothing to fear from this worm."

Focus: What Is the US Military Approach to Cyberwar?

In cryptography, a hash is a one-way function that creates a unique "fi ngerprint" of a fi le. The MD5 (Message-Digest algorithm 5) hash was a widely used way to add security by detecting tampering in fi les.

Focus: What Is the Chinese Approach to Cyberwar? "

"Never argue with a man who buys his ink by the barrel"

What about Deterrence in an Era of Cyberwar? "C

If you can't get what you want by attacking, then you won't attack in the fi rst place.

Why Is Threat Assessment So Hard in Cyberspace? I

1. The vulnerabilities that are most often targeted are the ones that no one but the attacker knows about.
2. Someone could be targeting your sys tems, but the goal might be to gather intelligence, steal information, shut down your operations, or just show off the hacker's capability. Threat assessment is about predicting the likely risks. But in cyber space, many of these risks will remain undiscovered until after an attack takes place.

Does the Cybersecurity World Favor the Weak or the Strong?

1. Examples like this lead many to believe that cyberspace is one of those strange places where the weak have an advantage over the strong. On one hand, the barriers to entry to developing cyberat

tack capabilities are relatively low, especially compared to build ing up more traditional military capabilities.

2. “Cyberspace grants small countries and individuals a power that was heretofore the preserve of great states.”
3. “One of North Korea’s biggest advantages is that it has hardly any Internet-connected infrastructure to target. On the other hand, the United States has tons of vulnerabilities a country like North Korea could exploit.”
4. This creates the strange irony of cyberwar. The more wired a nation, the more it can take advantage of the Internet. But the more wired a nation, the more it can potentially be harmed by those using the Internet maliciously.
5. Being powerful means you have the choice. Being weak means you don’t

Who Has the Advantage, the Offense or the Defense?

1. “The cyber competition will be offense-dominant for the foreseeable future.”
2. This means that crippling attacks out of the blue, the ultimate threat from the offense’s advantage, are not as easy to pull off in the cyber world as is often depicted.
3. “The attacker has to take a number of steps: reconnaissance, build a weapon, deliver that weapon, pull information out of the network. Each step creates a vulnerability, and all have to be completed. But a defender can stop the attack at any step.”

A New Kind of Arms Race: What Are the Dangers of Cyber Proliferation?

Are There Lessons from Past Arms Races?

while history may not always repeat itself, “It does rhyme.”

Behind the Scenes: Is There a Cyber-Industrial Complex?

Part III WHAT CAN WE DO?

Don’t Get Fooled: Why Can’t We Just Build a New, More Secure Internet?

1. To put it another way, the bigger the network, the more security problems, but the smaller the network, the less use ful it is.
2. As we’ve seen, separating secure and insecure sys tems by “air gapping” them is very diffi cult in practice, and hasn’t been a guarantee of safety.

Rethink Security: What Is Resilience, and Why Is It Important?

Reframe the Problem (and the Solution): What Can We Learn from Public Health?

1. For instance, botnets create a huge amount of infec tion across the Internet by spewing out spam, but they also make it hard to track down the more directed, malicious actors conducting more advanced cyberattacks
2. computers that are not protected or have been compromised with a bot put others at risk and pose a greater threat to society.”

Learn from History: What Can (Real) Pirates Teach Us about Cybersecurity?

1. To clamp down on piracy and privateering at sea, it took a two-pronged approach that went beyond just shoring up defenses or threatening massive attack
2. The fi rst strategy was to go after the underlying havens, markets, and structures that put the prof its into the practice and greased the wheels of bad behavior. Major markets for trading pirate booty were disrupted and shut down

Protect World Wide Governance for the World Wide Web: What Is the Role of International Institutions?

Countries have long sought to control the Internet within their own borders, both legally and operationally. As a report from the Internet Governance Project described, "That's why Bradley Manning is in jail and WikiLeaks is persecuted; that's why China constructed the Great Firewall; that's why South Korea censors Internet access to North Korea and vice versa; that's why France prosecuted Yahoo for displaying Nazi memorabilia."

"Graft" the Rule of Law: Do We Need a Cyberspace Treaty?

Understand the Limits of the State in Cyberspace: Why Can't The Government Handle It?

Cybersecurity is not a realm where the state can simply take over. Nor can it have "zero involvement" or "zero activity."

Approach It as a Public-Private Problem: How Do We Better Coordinate Defense?

1. Just as we saw with the worst threats in cyberspace, the best defenses against them rely on coordination.
2. These collectively built controls, which lay out the need for such measures as inven tories of authorized devices and software, and proper maintenance and analysis of audit logs, give any and every individual organi zation a set of clear security goals to follow.
3. his actions mattered because he mobi lized a network that could target key choke points by malicious actors in cyberspace.

Exercise Is Good for You: How Can We Better Prepare for Cyber Incidents?

1. "No plan survives fi rst con tact with the enemy."
2. Responses must be consid ered at every level, from national security strategy to enterprise risk management, down to the technical level, where engineers must make fast decisions about network incursions
3. "Test beds" are extensible simulations of systems, networks, and operational environments that can be attacked over and over again.
4. A particular tactic used by security researchers are "honeypots," or isolated machines that are intentionally exposed to attacks
5. These experts understand how to attack live networks in a controlled fashion, and lay the foundation for what might be a more damaging attack without putting the actual operation at risk.

6. As an illustration, one company that went through a war game studied by the McKinsey consulting fi rm found that their entire security team was completely dependent on e-mail and instant mes saging and did not have a backup communication plan to coordinate defense under a full-scale network-based attack.
7. Given the cost of these larger, more complex simulations, the designers must have a clear vision of the goals of the exercise and design the game appropri ately.

Build Cybersecurity Incentives: Why Should I Do What You Want?

Learn to Share: How Can We Better Collaborate on Information?

Demand Disclosure: What Is the Role of Transparency?

Get "Vigorous" about Responsibility: How Can We Create Accountability for Security? "

Find the IT Crowd: How Do We Solve the Cyber People Problem?

Do Your Part: How Can I Protect Myself (and the Internet)?

CONCLUSIONS

Where Is Cybersecurity Headed Next?

What Do I Really Need to Know in the End?