CHAPTER 1

WHAT IS (CYBER)SECURITY[1]?

■ ■ ■

Both technologists and lawyers have struggled to articulate what comprises cybersecurity—and what does not. Similarly, it can be challenging to differentiate cybersecurity from related terms such as data security, data protection, information security, and even privacy. This Chapter seeks to help you to begin to think conceptually about what cybersecurity is and is not. Without limits in our definition of the term, any legal question involving Internet technology could potentially be considered a cybersecurity problem. Cybersecurity spans a wide range of government and business functions and affects most sectors of the economy. We propose a formal definition for the term in Chapter 2, but for now, just consider what matters and what should be included in "cybersecurity."

A. INSECURITY IN THE WILD

We begin our introduction to the concept of (cyber)security with a series of examples. These scenarios are not intended to offer a formal definition of cybersecurity. Rather, they are selected incidents that meet two criteria: (1) the general consensus is they involve something called cybersecurity; and (2) they are of sufficient societal importance and impact to call for a policy response. Regardless of which substantive policy is ultimately applied by decisionmakers, these events matter.

1. CYBERSECURITY'S WILD HISTORY

We start with two historical anecdotes: what is likely the first compromise of a telegraph communications network, and the story of Lightning Ellsworth. Both of these anecdotes demonstrate that many of the themes of cybersecurity—and this book—can be disambiguated and stand separate from the newness of modern computer and communications technology.

The story of the Blanc brothers and the French mechanical telegraphs takes place in the 1790s:[2]

---

[1] We place "cyber" in parentheses because "security" as a field has long addressed many of the problems we examine in this text. However, the term "cybersecurity" reinforces internet connectivity as the source of many security problems.

[2] For more about this example, *see* Tom Standage, *The Crooked Timber of Humanity*, 1843 MAGAZINE (Oct. 5, 2017).

> The world's first national data network was constructed in France during the 1790s. It was a mechanical telegraph system, consisting of chains of towers, each of which had a system of movable wooden arms on top. Different configurations of these arms corresponded to letters, numbers and other characters. Operators in each tower would adjust the arms to match the configuration of an adjacent tower, observed through a telescope, causing sequences of characters to ripple along the line. Messages could now be sent much faster than letters, whizzing from one end of France to the other in minutes. The network was reserved for government use but in 1834 two bankers, François and Joseph Blanc, devised a way to subvert it to their own ends.

As a human operated, mechanical, system, operators would occasionally make mistakes during transmission, sending the wrong character. To account for this, the "alphabet" for transmission included the equivalent of a backspace character. The Blanc brothers took advantage of this feature to secure financial gain. They were bond traders in Bordeaux, where most trades were based upon information sent from Paris by mail. This mail took several days to get from Paris to Bordeaux. The Blanc brothers bribed a mechanical telegraph operator to encode information about Paris market conditions into telegraph messages, using the "backspace" character to ensure that their messages would go unnoticed as anything other than innocuous errors.

Their treachery was discovered after a couple of years. Curiously, however, they avoided any legal consequences, by virtue of the fact that there were no laws on the books that made their conduct illegal.

The story of Lightning Ellsworth is similarly engaging.[3] This story involves the electromechanical telegraph—the precursor to the telephone—which relied on human operators to tap out messages, typically using Morse code, that were transmitted as electrical pulses over copper cables. Individual telegraph operators tended to have unique patterns in how they tapped own messages. This afforded some level of security: the recipient of a telegraph message could usually recognize the cadence of each tapped-out message, which gave some assurances as to its authenticity.

George Ellsworth was a Confederate telegraph operator who was able to use this element of security to his—and the Confederate army's—advantage. He had a remarkable ability to mimic the cadence of other telegraph operators. He would travel with forward units and, as they encountered Union telegraph wires (the Union army devoted substantial effort to building out a telegraph network to use for wartime

[3] Stephen Towne, *The Adventures of Lightning Ellsworth*, N.Y. TIMES (Dec. 12, 2012).

communications[4]) he would attach a small device to the wires that let him both listen in on transmissions and tap out transmissions of his own. Ellsworth's ability to intercept messages was useful, but not entirely unique. His ability to mimic the cadence of other operators, however, gave him the unique ability to send false messages, for instance providing false reports of Confederate troop movements to distract Union forces.

2. CYBERSECURITY'S WILD PRESENT

Turning to more contemporary examples, we begin with Target Corporation's 2013 data breach. Then, we will discuss incidents with Yahoo, Inc., Wyndham Hotels, and the federal government's Office of Personnel Management (OPM).

In 2013, Target Corporation experienced a major data breach: over 40 million customer records, including personal and credit card information, were stolen from its systems.[5] The attackers were able to install intrusion software on the Point-of-Sale (POS) systems—that is, the physical cash registers coupled with payment card readers—used for card payments in Target's retail stores. As the POS systems process customer transactions, this attacker software, named KAPTOXA, monitors the systems' memory for valuable information like credit card numbers. KAPTOXA records this information and sends the data to computers controlled by the attackers, from which the information is collected.

How were the attackers able to install this software on Target's POS systems? The intruders stole network credentials from a contracting company, Fazio Mechanical Services, that serviced one Target location's HVAC (Heating, Ventilating, and Air Conditioning) systems. The store's HVAC computer network was connected to a central network that processed POS data. Unbeknownst to Target and Fazio, Fazio's own systems had been compromised. This gave the attackers a foothold.

Once this foothold was established, the attackers discovered that Target had not divided its network into subnetworks, which is a standard security precaution. This enabled the attackers to access multiple systems, not just the air conditioning unites with which Fazio needed to interact. Once the attackers accessed the store's central network using Fazio's stolen credentials, they could control the individual POS systems. Moreover, they could also directly access the Target corporate network, which allowed

---

[4] *See* Christopher Klein, *How Abraham Lincoln Used the Telegraph to Help Win the Civil War*, HISTORY.COM (Jul. 9, 2020).

[5] Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBS ON SECURITY (Sept. 21, 2015), https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/; Teri Radichel, *Case Study: Critical Controls that Could Have Prevented Target Breach*, SANS INSTITUTE (Aug. 5, 2014), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412; *Attacks on point-of-sales systems*, SYMANTEC (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf.

them to communicate with all of the company's other retail facilities. In one account, cited by security researcher Brian Krebs, it may have been possible for an attacker to compromise a (computerized) deli meat scale in one store and to leverage that scale to control a POS system in another store. This account is likely a dramatization of what happened in this specific incident, but is not outside of the realm of the possible.

Two of the questions we will focus on in this text is: *what could the organization in question have done to prevent the breach? Legally, who, if anyone, should be liable for any resulting damage?* Without a doubt, Target's network had problems; the lack of segmentation between various network systems is usually unwise. However, we now live in a world where POS systems, HVAC systems, and even deli meat scales are nearly always computerized and networked. Once a determined adversary is in the network, it's very likely that they will be able to find a path from the HVAC system to the POS systems.

Besides Target and the attackers, who else might be liable? What about other entities or individuals within Target's computer ecosystem, perhaps those responsible for developing the POS system(s)? Or Fazio, the HVAC contractor, which experienced its own breach resulting in attackers gaining unauthorized access to Target's system? The question of who to blame is difficult largely because the cybersecurity ecosystem—the network of various systems, parties, rules, and enforcement mechanisms—is incredibly complicated. Whereas in a typical commercial transaction various risks may be apportioned between a half dozen parties, in the cybersecurity context, risks may be apportioned between ten times as many parties, or even more. Ultimately, the relationships among risks, parties, and liabilities are far less clear than in the offline context. Furthermore, from the facts reported, we have no idea how private agreements, such as using contracts, might have allocated these risks between the parties. For example, Fazio might have made contractual security commitments to keep Target's credentials secure that it ultimately did not fulfill. Or, Target might have agreed to ensure that the HVAC system was securely maintained, and separated from the larger corporate network. A third party responsible for Target's network security might have failed to install appropriate firewalls between systems to segment the network. Without more information, it is difficult to clearly identify who is responsible from a liability perspective.

Curiously, when a breach occurs, we often look at the organization that had the relationship with affected individuals to identify responsibility. And yet, cyberattackers broke the law, accessed the systems, and stole and resold Target customer credit card data, without any pre-existing relationships with the stores' customers. In traditional civil actions over physical harms (typically the domain of tort law), such as lawsuits against parking garages or storage facilities, liability does not clearly fall upon the

facility operator in the event of a break-in. Physical structures generally are far less complex for analyzing liability than online systems. While this complexity might drive society to look immediately to the entity possessing the data, such as Target, the answer to the liability question is often far more complicated.

Target made mistakes, but many commentators argue that they had implemented reasonable security practices. Despite this, a number of lawsuits followed the breach, including breach of contract actions between banks that processed credit card transactions and the owners of those card brands (such as Mastercard or Visa), as well as customer tort actions. However, these lawsuits generally settled before trial, and thus without developing any significant case law that could guide future disputes.[6] The realities of litigating cybersecurity-related cases is another issue to which we will dedicate considerable attention because such lawsuits have proven very difficult to win. Notably, the Target breach was a one-time event. Target did not have a public history of security problems with its systems, and the attack that it experienced did not result from a failure to respond to prior incidents. Indeed, Target spent over $202 million remediating and managing the data breach, and after the breach, Target implemented extensive technology upgrades and bolstered its cybersecurity program. Many companies that experienced breaches during this period took similar post-incident steps.

There are many examples of firms whose security practices were lackluster, if not exceptionally poor. Yahoo! is perhaps the worst offender due to its repeated breaches: over three billion user accounts were compromised in the early 2010s, and Yahoo! experienced a breach again in 2016. After these breaches were made public, the New York Times published an article with the headline *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say*.[7] In addition to substantial legal costs, including settling a class-action consumer lawsuit for $117.5 million, Yahoo! experienced the first case of a sustained stock price decline.[8]

---

[6] Target has settled lawsuits with a wide range of plaintiffs. Jonathan Stempel & Nandita Bose, *Target in $39.4 million settlement with banks over data breach*, REUTERS (Dec. 2, 2015), https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203; Kevin McCoy, *Target to pay $18.5M for 2013 data breach that affected 41 million consumers*, USA TODAY (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/. In turn, in 2019, Target sued its insurance company to force it to reimburse costs of at least $74 million incurred in replacing credit cards due to the breach. Kavita Kumar, *Target sues insurer for up to $74 million in 2013 data breach costs*, STAR TRIBUNE (Nov. 19, 2019), https://www.startribune.com/target-sues-insurer-for-at-least-74-million-in-2013-data-breach-costs/565169292/.

[7] Nicole Perlroth & Vindo Goel, NEW YORK TIMES (Sept. 28, 2016), https://nyti.ms/2djkkel.

[8] *Here's How Much Yahoo Shares Are Dropping After Latest Hack Reveal*, FORTUNE (Dec. 15, 2016), https://fortune.com/2016/12/15/yahoo-shares-hack/.

Ultimately, Yahoo!'s security problems decreased its valuation by $350 million when it was acquired by Verizon in 2017.[9]

In other cases, firms have experienced repeated breaches and failed to respond to them. This was the case, as alleged by the Federal Trade Commission (FTC), with Wyndham Hotels. The FTC brought a regulatory enforcement action against Wyndham alleging unfair trade practices after hackers accessed Wyndham's systems on three separate occasions—and after Wyndham failed to address the underlying security problems. The Wyndham Hotel consent order, which memorialized the FTC and Wyndham's settlement, demonstrates how administrative agencies have the ability to impose cybersecurity program requirements:

> IT IS ORDERED that Hotels and Resorts shall, no later than the date of entry of this Order, establish and implement, and thereafter maintain, for twenty (20) years after entry of this Order, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data that it collects or receives in the United States from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall consist of the following administrative, technical, and physical safeguards appropriate to Hotels and Resorts' size and complexity, the nature and scope of Hotels and Resorts' activities, and the sensitivity of the Cardholder Data at issue.[10]

The Wyndham settlement raises another theme that we will consider this semester: what is the role of the government, such as federal administrative agencies, in ensuring cybersecurity? There are a number of models for enforcing (and defining) legal rights. For example, individuals may bring suit based upon contract law or tort law (that is, the law of wrongful harms); shareholders may bring suit based on misbehavior of officers or directors of a company; regulatory agencies like the FTC can establish and enforce rules on behalf of consumers; and prosecutors can bring criminal actions against bad actors. In later chapters, we discuss each of these approaches in turn, including their relative benefits and challenges.

Another example suggests that we may want to be cautious about relying on government expertise for regulating cybersecurity. In 2015, hackers believed to be connected to the People's Republic of China accessed the sensitive personal information of about 22 million government employees stored by the Office of Personnel Management (OPM). This

---

[9] Jeremy Kirk, *Yahoo! Takes $350 Million Hit in Verizon Deal*, BANK INFO SECURITY (Feb. 22, 2017), https://www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736.

[10] Stipulated Order for Injunction, *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 2:13–CV–01887–ES–JAD (D.N.J. Dec. 11, 2015), https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf, at 4–5.

information included comprehensive background forms on current and past government employees, including Social Security Numbers, residence history, family history, employment history, and further security clearance background check information. Hackers even accessed digital copies of fingerprints for 4.5 million employees, including active military and covert operations personnel. While not the largest data breach in recent history in terms of records, the breach of OPM's systems is surely one of the most devastating breaches in term of impact.

The OPM breach was also a result, at least in part, of poor security practices and failure to sufficiently respond to past security incidents. As reported by the House Committee on Oversight and Government Reform, attackers began exfiltrating data from OPM systems in July 2014—but were not detected until April 2015.[11] This followed years of reports citing substantial security problems. Since 2005, OPM's Inspector General had repeatedly raised concerns about the security of the agency's sensitive data. Surprisingly, the OPM breach involved two separate attackers. One was detected breaking into OPM's systems in March 2014, but was successfully locked out. While OPM technologists responded to the first attack, the second attacker was accessing the agency's systems using a different method. It took more than a year for OPM to find evidence of this second attacker.

3. CYBERSECURITY'S WILD WEST (OR, CYBERSECURITY IS HARD)

Despite these recent security problems, the federal government has some of the world's most sophisticated capabilities—both offensive and defensive. For example, organizations often contact the Federal Bureau of Investigations (FBI) after undergoing a cyberattack, especially when the attack is believed to originate in another country. In some situations, the FBI alerts private organizations when a data breach has come to the Bureau's attention through its own communication channels. Although the FBI does not overtly protect private organizations against cybersecurity attacks, the agency is an active partner in post-breach activities, such as by preserving evidence for later Department of Justice prosecutions.

---

[11] MAJORITY STAFF REPORT, THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION (Sept. 7, 2016), https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf. This report was largely produced by the Republican majority of the House Committee on Oversight and Government. The Democratic minority on the committee also released a memorandum critical of the Republican majority's conclusions, placing blame for the compromise of OPM's systems on government contractors and raising concerns that the majority report constituted a partisan attack on OPM's Democratic-appointed leadership. DEMOCRATIC STAFF, MEMORANDUM RE COMMITTEE INVESTIGATION INTO THE OPM DATA BREACH (Sept. 6, 2016), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-06.Democratic%20Memo%20on%20OPM%20Data%20Breach%20Investigation.pdf.

Multiple federal agencies have moved to regulate various aspects of cybersecurity, demonstrating the prevalence of and attention to problems with information technology security in recent years. This focuses generates an obvious question: if government entities are interested in cybersecurity, and have expertise to bring to bear, why do there continue to be so many cybersecurity problems?

The short answer is that it is remarkably difficult to design secure systems. Throughout this book, we will draw upon technical knowledge and business practices to describe these challenges, which help explain the complexity of regulating cybersecurity practices.

Consider three major recent security incidents that demonstrate the difficulty of doing cybersecurity well: the Heartbleed bug,[12] the Logjam bug,[13] and the DigiNotar attack.[14] All three of these incidents involve *encryption*. Generally stated, encryption is a way to mathematically transform intelligible data into unintelligible data. (The reverse process is called decryption.) Even if an attacker obtains encrypted data, they cannot read it. Under most state and federal laws, when an attacker accesses encrypted data elements but cannot decrypt them, there is no legal liability for the data breach—it is as though the attack did not occur. Practically speaking, the use of encryption does not eliminate the need for additional security techniques, such as limits on system access, but it reduces the overall risk of data loss or misuse. The combination of protective techniques used on a particular system or across a network provides cumulative security—what security professionals call "defense in depth."

Encryption remains, however, a critical part of most security strategies—albeit one of the most difficult parts to do well. Implementing encryption requires expertise, and designing encryption technologies is the realm of the most elite of these experts, so encryption-related incidents are truly remarkable.[15] The Heartbleed exploit was built upon a small flaw in the OpenSSL network security library—a piece of code that is at the heart of thousands of applications used by billions of people—that would allow

---

[12] *The Heartbleed Bug*, SYNOPSYS (June 3, 2020), http://heartbleed.com/.

[13] David Adrian et al., *Logjam Attack Proof of Concept Demonstrations*, https://weakdh.org/logjam.html.

[14] Hans Hoogarten et al., *Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach*, FOX-IT (Aug. 13, 2012), https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach.

[15] It is worth noting that none of these incidents involved a fundamental mathematical flaw in the encryption algorithm (i.e., a scientific flaw) but rather a failure to implement that algorithm properly. These can be distinguished by analogy to a combination lock: a *fundamental mathematical* flaw in the algorithm is like a combination lock that opens when something other than the correct combination is entered (e.g., if the combination "0 - 0 - 0" always unlocked it, regardless of what the manufacturer or user set as the purported combination). By contrast, an *implementation flaw* is similar to a lock that makes a distinct noise when the dial is turned to the next correct number in the sequence of the correct combination, and thus revealing the combination.

anyone on the Internet to read memory from any computers affected by the bug. Logjam is a bug in the Apache web server's implementation of the Diffie-Hellman key exchange protocol—a fundamental encryption tool—that made it relatively easy to break the encryption of web traffic. In the DigiNotar attack, hackers were able to compromise DigiNotar, a firm responsible for issuing and verifying the encryption certificates used to identify trusted parties on the Internet. This incursion allowed attackers to pretend to be anyone they wanted to be online, including, for instance, Google, Microsoft, or Citibank.

The most remarkable thing about all three of these incidents is that they affected core aspects of the cybersecurity ecosystem. OpenSSL, the Apache web server, and certificate authorities like DigiNotar provide basic pieces of architecture that are essential for the security of the Internet. Further, these technologies have been designed, implemented, and maintained by elite experts. If they can't get things right, how are average security professionals, let alone typical users, supposed to secure and maintain their systems?

QUESTIONS

1. What harm do users experience due to cybersecurity incidents? What if hackers obtain personal information about you, but they never share it? Or if they obtain and use credit card information, but the credit card company refunds those charges? How about if a hacker installs software on your TV that is used to "mine" bitcoins or other cryptocurrency[16] while the television is turned off? What if a hacker installs a program on your new car that causes the horn to briefly honk once when you turn the car on?

2. Tarony Home recently experienced a security incident in which their systems were compromised in a way that resulted in substantial and concrete harm to thousands of individuals. Did Tarony Home have bad security?

3. Social media platforms developed in the United States, such as Twitter and Facebook, were instrumental in bringing about a change in governmental regimes in Egypt in 2011, sometimes referred to as the Egyptian Revolution. Russia attempted to influence the 2016 U.S. Presidential Election in part by releasing information and creating fake news content that circulated on social media platforms. How are these incidents similar? Different? From the perspective of Egypt's fallen government, are they the same or different?

4. Some of the citations supporting the examples discussed above are to reports and whitepapers written by private firms such as FireEye, Infoblox, the SANS Institute, Akamai, and Fox-IT. Many of these firms are security consultants—they are in the business of selling security services. How does this affect how you read these reports?

---

[16] Bitcoin, cryptocurrencies, and blockchain generally are discussed in [[chapter]]. For now, it suffices to say that "mining bitcoin" (or other cryptocurrencies) is the rough equivalent of "printing money" using computer processing power, albeit money that is highly volatile in value.

5. As mentioned above, the Democratic Party minority on the House Oversight and Government Reform Committee wrote a counter-report criticizing the report issued by the committee's Republican majority. How might this affect how you read these reports?

6. a) You are a junior associate at a law firm. One day, during your lunch break, you spend a few minutes playing online poker. Soon thereafter you become concerned that someone is accessing the files on your computer, which include hundreds of sensitive client documents.

b) You try to install a new program on your home computer, of which you are the only user, but you are unable to do so because you are out of hard drive space. After a few minutes investigating, you discover a large folder containing thousands of files—including what appears to be a collection of child pornography. The dates on many of the files are quite old, but others are very recent.

c) While booking airline tickets for a trip to visit your family over the holidays, you discover that if you enter information into the airline's web page in a certain way, it books your requested tickets but does not charge your credit card.

In each of a)–c), what security concerns do you see? Who has engaged in objectionable activity? Who is responsible for that activity? What does "responsible" mean?

B. ASSETS & THREATS: CENTRAL CYBERSECURITY CONCEPTS

The real reasons why security problems exist are twofold: first, there are many motivations for exploiting these problems, so there is always an adversary waiting eagerly for organizations to stumble. Intruders attack cybersystems with a wide range of motives: for fun, prestige, money, to harm one's competitors, for domestic political reasons (e.g., activism, political protest), for foreign political reasons, or out of sheer boredom and curiosity. Second, human nature means that even when intruders are not nefarious by intent, or motivated to cause damage, they are still human, and humans make mistakes. Poorly secured Internet-connected systems are vulnerable to human errors that impact data confidentiality, integrity, availability, safety, or privacy in unexpected ways.

Two critical concepts for understanding cybersecurity are assets and threats. An *asset* is anything of value to an individual or organization that might be targeted by attackers or be vulnerable to threats. Although in financial language, assets are items that can be reduced to a pecuniary sum, assets in cybersecurity parlance are physical or logical things of value, broadly construed.

For example, assets to an organization could include employees, physical offices, computer hardware, computer software, and intangible

assets, such as intellectual property, trade secrets, proprietary information, or pure data. Assets can include personal physical property (moveable objects, such as computers or servers), physical real estate, people, and intangible property and data (what is stored in and transmitted between and within personal physical property). It is important to think broadly about assets, because assets are what an organization must protect, either because safeguards are required by law or because the organization seeks to preserve its financial investments or reputation.

Consider the Sony Pictures data breach of 2014. Attackers accessed Sony e-mail servers and released several internal e-mails to the public. These e-mails included embarrassing references to actors employed by Sony, damaging the reputation of the CEO and the company overall. Although sensitive personal information or trade secrets were not compromised, Sony would have preferred for these e-mails not to have become public. Assets in this case involved not only the e-mail server but also the contents of the messages. Organizations must identify which assets have value to the organization to make determinations about which cybersecurity protections a given asset requires and under what circumstances.

Many organizations implement a policy structure for internal cybersecurity requirements. This policy structure often includes a data classification regime or standard that categorizes data for purposes of specifying which cybersecurity requirements apply to particular data or system types. For example, sensitive personal information like biometric data might be required to be encrypted, while internal plans for marketing campaigns may not require encryption.

However, selecting the appropriate security approach has as much to do with the risks from potential threats as it does with the value of assets. Recall that without any attacker, human error, or natural disaster, assets would never need protection. Therefore, understanding the cybersecurity ecosystem means assessing both organizational or personal assets and who or what could compromise those assets. *Threats* are any potential event or action that may impact an asset negatively. Threats have three distinct aspects: the nature of their *relationship* to an organization, the *quality* of the threat source (or actual actor perpetuating the threat), and the *motivation* of the threat source. Understanding these differences helps an individual select an appropriate course of action for implementing a cybersecurity program and setting reasonable requirements.

The nature of the organizational *relationship* usually refers to the placement of the threat source. For example, threat sources are either internal or external to an organization—either part of the organization or outside it, such as a disgruntled employee (internal) and a foreign hacker (external). Further, the *quality* of a threat source may vary: threat sources may be people, or they may be a non-human events, such as a power surge

or an "Act of God," like a tornado. Finally, *motivation* matters. "Acts of God," for example, have no motivation. Employees who might make an inadvertent error are not nefarious or disgruntled. And a hacking organization may be primarily motivated by money. Different motivations inform what to protect and under what conditions. For example, if potential threat sources are financially motivated, they are more likely to attack large volumes of sensitive data that may be sold on the Dark Web, and less likely to access an organization's maintenance records.

Attacks are threats in action—when a threat source undertakes an intentional, nefarious action to harm an organization. One type of attack that is usually purely financially motivated is a ransomware attack. Ransomware is where attackers deliver malware to a user, such as a link or an attachment in a phishing e-mail. After the user downloads the file or clicks on the link, the ransomware encrypts sensitive data on the user's computer, making it unusable, or held for "ransom," until the individual or an organization pays a specific sum. Attackers will only decrypt the data in exchange for payment, and frequently attackers threaten to destroy the data unless the payment is made within a prescribed number of hours or days. Targeted organizations that do not pay the ransom frequently cannot recover their data.

After the target individual or organization transfers money to the attacker (generally using cryptocurrency), the attacker provides them with a decryption key to recover the encrypted data. Many different organizations have been affected by ransomware, from large municipalities and healthcare organizations to law firms and other small businesses. The amount of money demanded is usually based on the data type, repository size, and importance, as well as the buying power of the organization. While an individual might only have to pay a few hundred dollars, law firms or other small businesses might have to pay in the hundreds of thousands, while large companies may have to pay millions.

For law students, it is worth noting that law firms have recently become important targets for attacks. Law firms have a poor history of cybersecurity and their computers often contain large amounts of sensitive and crucially important information from many clients. This makes them valuable targets. Attackers rarely care about harming the law firm. Rather, attackers care about using the information managed by the law firm for financial gain (e.g., insider trading[17]), to help an adverse legal party, or for political purposes (this is less common but, as the Panama Papers makes clear, is a real risk[18]).

---

[17] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL STREET JOURNAL (Mar. 29, 2016), http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[18] *The Panama Papers: Exposing the Rogue Offshore Finance Industry*, INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS, https://panamapapers.icij.org/; Luke Harding, *What*

Another important attack motivation for hackers is to obtain control over systems that they will then use in their future activities. Sometimes hackers obtain control through graduated steps. During the Target data breach, for instance, the attackers first compromised an HVAC vendor. The credentials gained from the vendor provided an entry point into the rest of the Target network. Other times, the compromised system becomes a tool in the attacker's arsenal. On October 21, 2016, attackers used a network of roughly 100,000 compromised Internet-connected security cameras to launch a Distributed Denial of Service (DDoS) attack on Dyn, a company that provides Domain Name Server (DNS) and other infrastructure services to large parts of the Internet.

If DNS and other infrastructure services are interrupted, websites may not be available, impacting business and other operations. As a result of the Dyn attack, large parts of the Internet in the United States were inaccessible to users for much of the day. Importantly, this attack was facilitated using a network of several thousand compromised computers, yet these attackers had zero interest in "pwning"[19] individual computers with any motivation other than to create a network that could target Dyn.

In the following chapters, we will consider these and dozens of other examples as tools for looking at the issues highlighted above and many others.

QUESTIONS

1. Are you surprised by the wide variety of things that are considered assets? Without yet knowing details about security techniques, what do you think might be some of the differences between protecting a physical object, like a server, and protecting intangible data?

2. Organizations often begin the cybersecurity process by creating a "data flow diagram." What do you think the value of such a diagram might be? Using your internal home network, can you diagram how data flows from your device to your router, and to your ISP?

3. What are some of the differences among threat sources? Can you think of circumstances where internal threats might be a greater concern than outsider threats?

C. ("CYBER")SECURITY "LAW"?

"Cybersecurity law" lacks a clear definition; indeed, there is debate over whether such a field even exists. This may seem a problem for a class

---

are the Panama Papers? A guide to history's biggest data leak, THE GUARDIAN (Apr. 5, 2016), https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.

[19] *Pwning* (pronounced "own-ing") is the act of using a computer in an unauthorized manner to achieve specific goals related to the exercise of control, such as creating a DDoS attack network or encrypting a computer using ransomware.

that focuses on cybersecurity law and policy. Some also argue, at least partially in jest, that there is no such thing as cybersecurity policy, either. This glib assessment is, of course, not accurate, though it is correct to say that our approach to cybersecurity policy is in its infancy and that cybersecurity policy five years from now likely (hopefully!) will look very little like it does today.

To be sure, there are cybersecurity *laws*. There are also informal and "soft law" rules that apply today, such as norms, guidelines, best practices, and policies, some of which have been developed in response to cybersecurity concerns, and others of which were simply inherited from different contexts of varying relevance. There are also many practical cybersecurity concerns that lawyers face, from the cybersecurity issues that law firms confront as businesses, to the practical guidance a lawyer gives her clients about their security, to the new and unique ethical issues that draw upon existing norms and legal models, including the common law, statutory language, and administrative behavior.

Instead of surveying all cybersecurity *laws*, this book provides a wide base of knowledge and perspective about technology, cybersecurity principles, and legal principles that affect the field. Survey approaches can be useful in well-established fields or fields where studying the range of existing law is helpful to learn the deeper concepts that define the area. Neither of those is true of cybersecurity today. Therefore, we do not attempt to provide a comprehensive list of all legal regimes that could be considered cybersecurity laws. Rather, we offer examples and legal concepts.

Discussions of cybersecurity today recall the debate between Judge Frank Easterbrook and Professor Lawrence Lessig nearly two decades ago over whether there was value in studying cyberlaw. Judge Easterbrook argued that cyberlaw is akin to the "law of the horse," explaining that:

> Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students—better, even, for those who plan to go into the horse trade—to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader

> rules about commercial endeavors could one really understand the law about horses.[20]

Lessig responded that there was something different about cyberspace that made its study worthwhile. He explained:

> I agree that our aim should be courses that "illuminate the entire law," but unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect.
>
> This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace, comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. . . . The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law's regulation outside of cyberspace.[21]

The past twenty years have delivered a mixed verdict in favor of Lessig. An important aspect of his argument is that the underlying characteristics of "real space" and cyberspace are somehow different.[22] This idea has not necessarily aged well: if anything, over the past decade the online and offline worlds have increasingly merged (a transition that has had important impacts on security), as a large portion of our personal and work lives have moved online. At the same time, the idea that there is something important to be learned about the law in general through the study of "cyberlaw" has proven quite sound.

Studying cybersecurity is the next step in the project Lessig articulated. When he began, the online and offline worlds were distinct. This made study of their differences valuable, both for the specific rules that govern conduct in each and for understanding the law generally. But today these worlds are colliding. That merger creates new risks for the offline world.

What makes cybersecurity *cyber* instead of just *security*? Adding the cyber prefix to just about anything is, of course, a common trope. It is a

---

[20] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 UNIVERSITY OF CHICAGO LEGAL FORUM 207 (1996).

[21] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harvard Law Review 501 (1999).

[22] The core thesis of much of Lessig's work is that "code is law"—in cyberspace, rules that govern how individuals interact are defined by the computer code that creates the cyberspace. Because cyberspace may be subject to the equivalent of different physical laws than the real world, we should expect that conduct online will be different from—and properly subject to different rules from—conduct offline.

largely meaningless way of modernizing otherwise stale content for the modern world. Anytime you take something that you already do offline and start doing it online, you're "cybering"—you're doing something new and exciting! Or so you think. More accurately, or, perhaps, more cynically, you're just using a computer to do whatever you were doing before. More often than not, adding the cyber prefix to an activity illustrates a lack of understanding about the internet and its pervasive nature.

But in the context of security, the "cyber" component really is doing something important.[23] Security is about managing risk: identifying threats, assessing exposure to harm from or vulnerability to those threats, and finding ways to avoid, reduce, or absorb that risk. When conduct moves from the real world to cyberspace, whole new classes of threats and vulnerabilities come into play. Cybersecurity is not merely "security in cyberspace." It's the study of how and why the transition to cyberspace changes the risk calculus, and how to respond to these changes.

Cybersecurity law is a young field. In 2011, Professor Joseph S. Nye Jr. compared the state of cybersecurity policy to that of nuclear policy in the 1950s:[24]

> Political leaders and analysts are only beginning to come to terms with this transformative technology. Until now, the issue of cyber security has largely been the domain of computer experts and specialists. When the Internet was created 40 years ago, this small community was like a virtual village of people who knew each other, and they designed an open system with little attention to security. While the Internet is not new, the commercial Web is less than two decades old, and it has exploded from a few million users in the early 1990s to some two billion users today. This burgeoning interdependence has created great opportunities and great vulnerabilities, which strategists do not yet fully comprehend. As Gen Michael Hayden, former director of the CIA says, "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]. . . . I have sat in very small group meetings in Washington . . . unable (along with my colleagues) to decide on a

[23] Perhaps the best criticism of the term cybersecurity is that it focuses attention on the technological, computer, and network components of the ecosystem, distracting from other equally important components. For instance, and as we will see throughout this book, physical security and operational security are critically important to a good cybersecurity posture. As explained by Professor Andrea Matwyshyn, "[r]eferring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NORTHWESTER UNIVERSITY LAW REVIEW 795, 817 n.99 (2013). Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. *Id.*

[24] *Nuclear Lessons for Cyber Security?*, 5 STRATEGIC STUDIES QUARTERLY 18 (2011), https://dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf.

course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make."

Governments learn slowly from knowledge, study, and experience, and learning occurs internationally when new knowledge gradually redefines the content of national interests and leads to new policies. For example, the United States and the Soviet Union took decades to learn how to adapt and respond to the prior revolution in military affairs—nuclear technology after 1945. As we try to make sense of our halting responses to the current cyber revolution, are there any lessons we can learn from our responses to the prior technological transformation? In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy.

Nuclear policy is an interesting point of comparison as we begin to discuss the challenges in an inherently adversarial system. Although physical risks can be used to better understand the nature of cybersecurity risks, the physical environment differs, at least in part, from the unique challenges of cyberspace.

QUESTIONS

1. How is the "real world" different from cyberspace? What does it mean for someone to violate your security online versus offline?

2. Based on what you read above and otherwise know about nuclear technology, how is cybersecurity similar to and different from nuclear security?

3. How do law and technology relate to one another when it comes to studying and practicing cybersecurity? What does it mean to "practice cybersecurity"?

D. A NOTE ON TERMINOLOGY AND NAVIGATING THIS TEXT

Cybersecurity is a field with a great deal of specialized terminology with technical meaning. We, unapologetically, eschew much of this specialized meaning. We do so particularly where terminology is territory, where adherents to a particular usage insist upon technical accuracy because the term has a precise meaning to them rather than because it has a generally useful meaning. We do use terms that are necessary to communicate certain concepts within cybersecurity.

We take this approach with some reluctance and out of necessity. Meaningful discussion of cybersecurity as a distinct field requires bringing

together multiple constituencies, often from across disciplines. This is not possible unless each constituency acquiesces to speak some common vulgar tongue.

Some perspective on our approach is captured in the excerpt below. This is a portion of Peiter Zatko's address at DEFCON 21 in 2013.[25] Zatko is better known as Mudge, one of the founding members of the L0pht,[26] a famous hacker think tank formed in 1992, and a member of the hacker group Cult of the Dead Cow. In 2010, Mudge "went legit," accepting a position with the Department of Defense (DoD) overseeing cybersecurity research at the Defense Advanced Research Projects Agency DARPA). In this excerpt, Mudge discusses the clash of cultures, language, purpose, and generally understanding between the DoD and the hacking community:

PEITER ZATKO A/K/A MUDGE, UNEXPECTED STORIES FROM A HACKER INSIDE THE GOVERNMENT

DEFCON 21 (2012)

I remember Anonymous from way back. I mean—Anonymous—I use it as like, you know a proper noun, but obviously we're all familiar, and it's much more. It's kind of a movement, a thought, it's more ephemeral than that. And when I remember them, they were going after Scientology, and RIAA and there was all the 4chans with the soap opera stuff going on. And at some point, their scope or the target expanded to include the government. And general wisdom was that the triggering event was the DoD's response to Wikileaks and [Chelsea] Manning, etc. But the way I saw it, there was actually something else that was a bit more subtle that folks hadn't realized.

So, in 2011, the DoD released the strategy for operating in cyberspace. There was some very minor backlash to some of the wording initially, I think there was an initial small leaked version of it that went out and it was followed by a later one. But there was some more specific backlash and chatter in the hacker researcher community. The strategy stated that the DoD was going to treat cyberspace as a domain to conduct operations in. And it appeared kind of modeled off of outer space, you know, treating space as—these are "DoDish words"—a domain. And there were some confused conversations going, "Oh, why is anybody upset if the treat cyberspace as a domain, there wasn't that much upset with treating space [as a domain,] and you know, nobody lives in cyberspace," which you could kind of only hear inside the government, a statement like that. Because if you think about it, you know, we all live in cyberspace. And the hacker

[25] A recording available at https://www.youtube.com/watch?v=TSR-b9yuTbM. This excerpt starts at approximately the 11:30 mark.

[26] For some introduction to the L0pht, including to Mudge, and their groundbreaking testimony before the United States Congress in 1998, *see* Craig Timberg, *A Disaster Foretold—And Ignored: L0pht's Warnings about the Internet Drew Notice but Little Action*, WASHINGTON POST (June 22, 2015).

researcher community made it—you know, made cyberspace—(I'm really not a fan of that word)—made the Internet an online our homes well before the government and everybody else kind made it just where they always lived and did everything in.

So if you send a message that that's somebody's back yard and that you're going to militarize and prep for war in somebody's backyard, that can sound really scary, and it can galvanize folks to respond. One of the problems was there was not an understanding as to who the message was actually intended for. So in addition to treating it as a domain, they said something else, which was, and in response to—and I'm paraphrasing—and in response to hacks, we'll consider responding with kinetic force.

So, if you don't actually specifically call out who the recipient of the message is, everybody reading it thinks it's directed to them. I read it. I thought it was directed to me. And I'm going like, you know, "What the heck?" You know, I joke, my buddy and I replace his, you know, the HTML, the main Web page, and that' considered a hack, and all of a sudden I've got somebody launching a Patriot missile at me? I mean, this makes no sense. What level of hack? Because if we look at like CFAA response, maybe they actually thing a Patriot missile is the right thing for defacing a Web site. I don't know. And none of these are the right questions. Because I'm not the intended audience. But of course, I'm reading it as if I was. And of course, the logical next question is, wait, do they understand how attribution works? Because, you know, what if I do it, you know, bouncing through an ally? What if I do it from within the U.S.? Are they going to kinetically respond against themselves? I mean, this is. . .

You kind of go, ok, wait. Back up. If the message were directed to, let's say, other countries, other. . . somebody in specific that's got a significant power that they say, look, we're talking about critical infrastructure, or something of that nature, if you turn off the lights in New York, we will probably be able to figure out who you are, because you're not a small little hacker defacing Web sites, and maybe there is attribution in place that we could respond to. That would have been an entirely different sort of message, and I wouldn't have read it as the whole like, wow, if I get root on something in my own system, is the Government going to shoot me? Which is just silly. But I wasn't the only person who read it that way. And it's nice having been in this field and in the hacker researcher community for, jeez going on almost 25 years. Actually, over 25 years. And some folks were sending me, they're like "Hey, have you seen what's going on in the chat rooms?" And there were some folks who were claiming affiliation of claiming support of Anonymous that were going "Hey, have you read this? Look who's trying to prep for war in our back yards. Do they even understand how attribution works? This is bullshit. If they think they can find me, it's on. Let's go."

And the next thing you know, there are a couple websites defaced, and they ended in .gov. Now, this is where it gets kind of funky. Defacing a website is kind of a message. It's a little warning shot. But that's in a language that govies don't know. So the govies didn't get the message, as far as, you know, what I saw. So here's the initial strategy for operating in cyberspace that goes out, probably directed to somebody else, but by poor messaging, is misinterpreted by a group. The group responds, fires a warning shot. The warning shot isn't understood. It's like, "Hey, what are these vagabonds doing? Look at the little street punks or whatever. They're not somebody who actually has a message that we should actually engage in." And it's just this little cascading effect.

So, that is kind of unfortunately where I saw, you know, the expanding of scope and a lot of misunderstandings. I'm not saying the two groups should be friends. And I'm not saying one group is good and one group is bad. But when you send a message out into the world, and this is for both groups: you really need to make sure it's understandable by all the parties that are going to receive it. You can't assume it's just going to be read by the person you had in mind. With all love and respect, there is one very obvious commonality between the hacker researcher group and the government, and it's that they can be very arrogant and expect that everybody will speak their own language and that they don't have to speak anybody else's. And I think that's a really common mistake.

So the recommendation for the government from my vantage point on both sides is: figure out how your messages are going to be received by the more general populace of cyberspace, because we all live there now. This is actually a great opportunity for diplomacy. You can kind of think of it like the Lost City of Atlantis. Because cyberspace kind of took the world, I think, the world by surprise. Obviously it hasn't been around that long. So what if Atlantis just popped back up, and there was an advanced, very technically capable group of people there? You wouldn't sit there and ignore them. You wouldn't taunt them. You wouldn't attack them. You'd probably actually try and understand them and figure out how messaging to somebody else might be interpreted to them. You might even try to figure out where you guys already see things eye to eye, and where you have differences.

So, my recommendations to the citizens of cyberspace is: keep in mind that the government and in particular, the DoD, has very specific focuses and goals. And they often only see things from their own point of view. Because they're really focused on doing that job. And when you read things that appear to be a message directed to you or your community, coming from an unlikely source, you should question whether or not the message is actually intended for you, or if it's just intended for somebody else and really poorly worded. And if you still think a response is necessary, you

really need to think about the message that you're sending, to make sure that you don't make the same mistake in return.

Mudge identifies a critical challenge for cybersecurity as a field: a lack of common terminology. As is clear from his account, the emphasis there must be on the word *common*. Many individuals in many fields are working from many perspectives on things that can be called cybersecurity. But these myriad perspectives do not share a common understanding or language for the field, and sometimes describe similar things in different terms and different things in similar terms.

This lack of a *common* terminology explains in part our unapologetic if reluctant approach to terminology. Anything else would be impossible—we would necessarily be cabined into a single perspective, to the exclusion and marginalization of other perspectives. That would run directly contrary to the interdisciplinary ambitious of this book.

But there is another, more fundamental, reason that we eschew the language of any particular perspective on cybersecurity. Many fields claim cybersecurity as their own. DoD and the National Security community stake a claim to cybersecurity; engineers stake a claim to it; the business community has a claim to it as well; and, of course, lawyers claim all as their own as well. It is our perspective, and hope, that cybersecurity is coming into its own as a field—and that this book contributes to that development.

At the same time, we are not prescriptive about our choice of language, instead opting for a dialect that blends the terminology and perspective of these various constituent fields. This choice, too, is deliberate, because cybersecurity has not yet emerged as its own field. Rather, to successfully work in cybersecurity's broad domain, you should have some fluency across its constituent fields. From this perspective, our dialect is intended to familiarize readers with the terminology that one is likely to encounter in these various field. That is, regardless your own background, you should have some fluency in the language that engineers, business professionals, and lawyers use when discussing cybersecurity.

Dan Geer, one of the leading thinkers in this field, offered some relevant reflections that bear on our thinking about the language of cybersecurity, and the bearing that language has on cybersecurity as a field:[27]

[27] A recording, and text, of Geer's talk is available at https://www.usenix.org/conference/satcpi15/meeting-program/presentation/geer.

DAN GEER, *T.S. KUHN REVISITED*

NSF, Secure and Trustworthy Cyberspace
Principal Investigators' Meeting (2015)

"Does a field make progress because it is a science,
or is it a science because it makes progress?"

As you know, I chose for my topic today a re-visitation of T.S.Kuhn's landmark work, *The Structure of Scientific Revolutions*. I rather suspect many of you have read it, and, if so, most probably as an assigned reading in your preparation for a career in science. It was published in 1962 by the University of Chicago as a volume in the International Encyclopaedia of Unified Science, a project that was never, in fact, completed. [. . .]

Kuhn's book, which he consistently refers to as an essay, is basically about what science is, based on the observables of what science does and has done. Between him, his supporters and his critics, many noted philosophers, and others, what science *is* is to this day unsettled at its core. Perhaps that is why both Kuhn's supporters and his critics agree on one thing: There is no algorithm to science. [. . .]

Biases aside, the time has come to read Kuhn's essay in the context of cybersecurity. He begins and ends with what is a circular idea, that a scientific community is defined by what beliefs practitioners share, and what beliefs practitioners share defines what community they are in. This is, in fact, instructive as no science begins in mature form, but rather any new science will begin in much more modest circumstances where, in fact, there is nothing approaching a consensus in any sense of the word, that, early on, consensus is not even a concept. As such, part of becoming a mature science is the development of a broad consensus about the core concerns of that branch of knowledge.

Kuhn's word for the collections of exemplars of good science was "paradigm," a word whose meaning today is all but entirely Kuhn's . . . .

But what is a "paradigm" and why do we want one? As Kuhn puts it, "[Paradigms] are the source of the methods, the problem field, and the standards of solution accepted by any mature scientific community at any given time." Kuhn's book and the two decade long back and forth between Kuhn and philosophers notwithstanding, the simplest version is that a paradigm is all the things that a scientist can assume that his or her colleagues will congenially understand about their common work without explicitly explaining them or arguing them from first principles again and again.

Several authors besides Kuhn have adopted that idea to explain the proliferation of jargon as being something that markedly improves the efficiency of communication between practitioners who do, in fact, share a paradigm, who share a set of techniques, trainings, and world view in common. As Kuhn said, "Although it is customary, and is surely proper to

deplore the widening gulf that separates the professional scientist from his colleagues in other fields, too little attention is paid to the essential relationship between that gulf and the mechanisms intrinsic to scientific advance." In other words, impenetrable jargon between scientists sharing a paradigm is a side-effect of that sharing, and a tool of efficiency because it insulates science from society.

But, I hear you say, any field from poetry to American history to macroeconomics can have an impenetrable jargon, does that make those fields sciences? Clearly not, and here is where Kuhn's paradigm construct is central. In a science, the shared paradigm is universal whereas in the humanities, say, there are always competing schools of thought that are unlikely ever to sign some unifying intellectual peace treaty. As Kuhn would have it, a paradigm—a shared framework for how the world works—is the engine for creating the kinds of puzzles that individual scientists are able to solve if they work hard enough, the paradigm creates general agreement amongst those who hold it as to where further research is needed. When a body of scientists is asked "Where should research go next?" the answer will be the same as to the question "Where is research going?" because the shared paradigm makes it so. And note that I used Kuhn's word, "puzzles," rather than "problems." Kuhn is at some pains to make clear that a scientist doing science is solving the puzzles that the paradigm leaves open to solution. He or she is not solving problems in the vernacular sense of the word "problem." [. . .]

———

It is both the conceit and concern of this book that there is, or at least should be, an interdisciplinary field of cybersecurity. This is reflected in the subtitle of this book: "An interdisciplinary problem." As Geer suggests, there is a distinction between the puzzles that drive the work of an established science and the problems that drive a yet-inchoate field. We believe that there is a common set of issues to be addressed by an interdisciplinary cohort of researchers, practitioners, and policymakers, sharing a common language to puzzle through something called cybersecurity.[28]

[28] Those familiar with Kuhn's work, or who read the entirety of the address from which Geer's excerpt above comes, will be familiar with the idea that crises are the force that drive the development of new paradigms. Crises result, for Kuhn, where existing paradigms encounter "puzzles" that they lack the vocabulary to address—that is, problems, not puzzles. This failure of existing paradigms forces a refactoring of fields, to develop a new vocabulary that is capable of rendering these newly incomprehensible problems into comprehensible puzzles.

The language of "crisis" may be dramatic to describe the formation of a new scientific field. At the same time, the challenges posed by cybersecurity to nearly every aspect of modern life and society, and the failures of any current field to address these challenges in a consistent, timely, or predictable way, suggest that it may well be fair to describe the current state of the field as a crisis.